JRSR
JOURNAL OF REGIONAL STUDIES REVIEW

Journal of Regional Studies Review (JRSR)
Volume 4, Issue 2 (Spring 2025) | Pages: 92–104
ISSN (Online): 3006-6646
Digital Object Identifier (DOI): 10.62843/jrsr/2025.4b115
Correspondence should be addressed to Musa Khan; musakhan_85@yahoo.com

RESEARCH ARTICLE

# Digital Hybrid Warfare (7GW): Threats to Pakistan's Security and a Framework for Countermeasures

Muhammad Zia Ul Haq [a] Musa Khan [b]

**Abstract:** The aim of this study is to explore the emerging phenomenon of 7th Generation Warfare (7GW) and assess its implications for Pakistan's national security landscape. Rooted in the evolving landscape of media hybrid warfare, 7GW operates through non-kinetic means, including cyber-attacks, disinformation campaigns, artificial intelligence applications, electronic, cyber warfare and the use of space and drone technologies. The paper examines how these advanced tools are employed by both state and non-state actors to destabilize Pakistan's institutions, manipulate public perception and exploit societal divisions. Utilizing qualitative research methods, including semi-structured interviews with key stakeholders, the study examines existing literature, recent cyber incidents, and hybrid warfare patterns targeting Pakistan. To guide this analysis, the study employs a composite theoretical framework drawing from the Revolution in Military Affairs (RMA), Hybrid Warfare Doctrine, and Information Warfare/ Cognitive Domain Theory, which collectively illuminate the strategic, technological, and psychological dimensions of 7th Generation Warfare (7GW) as they manifest in the Pakistani context. It identifies the strategic vulnerabilities within Pakistan's information, cyber and national security frameworks. The findings reveal that 7GW is a multidimensional threat that bypasses traditional battlefield paradigms and requires an integrated response strategy. The study proposes countermeasures including the strengthening of digital infrastructure, development of national cyber defence policies, media literacy initiatives and investment in technological innovation. The paper concludes that a comprehensive understanding of 7GW is essential for formulating robust national security policies in the age of digital conflict.

**Keywords:** 7th Generation Warfare, Hybrid Warfare, Cybersecurity, Media Warfare, Pakistan National Security, Artificial Intelligence, Disinformation, Non-Kinetic Threats

## Introduction

We live in an era of technology: witness the amazing developments currently occurring and how fast they are unfolding. However, the use of today's digital technology for military purposes is much more significant than in yesteryear. Generation Seven Warfare is a relatively new concept describing non-real warfare that occurs in the digital space (Muhammad Usman, 2024). Advanced Technology Leads the Tactics in Other Aspects: For example, Hybrid Media Warfare (HMW), a term recently designed and introduced that embodies both traditional and non-traditional tactics to weaken and eventually destroy a social structure from without as well as from within. Characterized by the use of public opinion warfare, cyber warfare and other equally inconspicuous means to wage a quiet storm against an adversary it can be difficult for him/it to recognize or defend against. To Pakistan's national security, 7th-generation warfare poses a huge threat. In recent years, Pakistan has suffered cyber attacks and disinformation campaigns, targeting its government, military and people (Fazal, 2022). These attacks originated with both state and non-state actors and caused damage

[a] PhD Scholar, Riphah Institute of Media Sciences (RIMS), Riphah International University, Islamabad, Pakistan.
[b] Associate Professor, Riphah Institute of Media Sciences (RIMS), Riphah International University, Islamabad, Pakistan.



Cite this Article: Haq, M. Z. U., & Khan, M.(2025). Digital Hybrid Warfare (7GW): Threats to Pakistan's Security and a Framework for Countermeasures. *Journal of Regional Studies Review, 4*(2), 92-104. https://doi.org/10.62843/jrsr/2025.4b115

that destabilized the country (Khan, 2023). Pakistan is also threatened by propaganda and disinformation warfare from neighboring states like India.(Warrich et al., 2021).

Within this context, 7th Generation Warfare (7GW) characterized by its non-kinetic, information-centric, and technologically sophisticated nature represents an escalating threat to Pakistan's national security (Nadvi & Nadwi, 2022). National security refers to the protection of a country's sovereignty, territorial integrity, citizens, economy, and way of life from threats both internal and external. It encompasses a wide range of activities, policies and measures that aim to maintain the safety and well-being of a nation and its people. The concept of national security includes a range of different elements, including military defense, intelligence gathering, information analysis, border security, counterterrorism and law enforcement, cyber defense, economic stability with growth, social welfare, human development, diplomacy, and foreign relations (Abbas Awan & Javaid, 2020). National security of Pakistan is an issue of critical importance to the country given its strategic location and history of regional conflict, Pakistan faces a range of internal and external threats to its sovereignty, territorial integrity, economy, and way of life (Baber, 2020). To ensure national security, some of the major elements are to maintain a strong military and intelligence force; to promote economic development and stability; to invest in infrastructure and social services; to keep our borders and ports well defended and free from crime; to fight terrorism and extremism; and to develop strong alliances with other countries and international organizations (Ogden, 2020).

Pakistan has been involved in regional wars for a long time. It spent much of the 1950s fighting with its neighbor India over the contested territory of Kashmir. In the 1980s, it was one of a number of countries that supported Afghanistan's Mujahedeen forces against the Soviet-backed government in Kabul under President Najibullah. But when Moscow withdrew its troops in 1989 in order to pave the way for peace talks between warring factions on both sides of that conflict, Pakistan alone ventured into new and uncertain terrain without having any clear formula about how best to restore some kind of order to areas such as Pakistan's tribal areas where hundreds had died during years of war between the two superpowers, or what might happen on its own doorstep if events there went uncontrolled(Sultana et al., 2021). Cyberwarfare, internet-detained conflicts and other forms of seventh generation warfare appearing in recent years have put great challenges on Pakistan's national security. Seventh generation warfare capitalizes on technology and the digital domain to secure strategic goals. It is often waged by non-states and other groups without traditional military capability (Bris et al., 2021). The main challenge of 7th-generation warfare is that it can spread disinformation and propagandise on social media and other online platforms, causing the public to be confused and distrustful. This type of war can be used to incite violence or destabilize the political system. It is indeed a dilemma for Pakistan to combat this disinformation( spelled out ), particularly disinformation campaigns emanating from unfriendly neighbors (Sultana et al., 2021).

Another challenge of 7th generation warfare is its ability to disrupt basic infrastructure and communication networks, causing significant economic loss, or interference with governmental capacity to deal with emergencies and maintain public order. Pakistan has suffered several high-profile cyber-attacks in recent years, including attacks on banking and finance systems, power grids and other indispensable infrastructure (Fazal, 2022). Finally, terrorist organizations and extremist groups exploit 7th generation warfare in order to gain strategic advantage. This may mean using social media and internet platforms to recruit new members, co-ordinate attacks and disseminate propaganda . Pakistan has faced significant challenges in countering these groups that have taken root on its border with Afghanistan. To meet these challenges, the government and military of Pakistan have taken a series of measures including enhancing the country's cyber-defense capabilities, upgrading its ability to collect and analyze intelligence data, tightening supervision in border areas as well as cooperating with other countries to fight terrorism and extremism. To continue taking these actions and maintaining a strong defense against the threat posed by seventh generation warfare is of vital importance for Pakistan (Ali, 2024).

Though the dangers that Media Hybrid Warfare ("MHW") poses in general are commonly acknowledged, a significant hole in understanding is escaped when it comes to being able to say how key Pakistani actors experience, hurt and benefit from 7GW. As a constituent part of broader phenomenon (MHW). Furthermore as for now, by constantly looking for motion instead of rest and abstracting from this movement more efforts need to be made to collect the views of stakeholders in a systematic way in order to work out how exactly 7GW within Media Hybrid Warfare should be treated specifically (Matloob et al., 2023). As long as the finer points of this hybrid warfare phenomenon remain unclear, Pakistan will be handicapped not only in playing the hand of a proactive strategy where it comes to those sophisticated campaigns against public trust which go by one of its key elements such as "shape a message," but also whenever information manipulation of national narratives depicts the country's image badly. If a fall could lead to chaos and unsustainable infrastructure over wide areas take place for even just some of them how much more powerful (Matloob et al., 2023) would he become on account of having sown chaos in these strategic roots across an entire region instead? Hence state This research aims to fill this critical gap by assessing how key Pakistani stakeholders (authorities, opinion leaders, etc.) perceive 7GW part time broadcasting-as-of-war articulated within a the M-Hybrid Warfare whole, and also to intelligent and informed stakeholder-driven strategies for correct doing aways with or at least effectively resist those latest menaces of our age arising against national resilience (Geissler et al., 2023; Richardson, 2023).

In light of the above context, this study particularly addresses the following research questions: first, how do key stakeholders in Pakistan perceive and assess the specific challenges posed by 7th Generation Warfare tactics as an integral component of Media Hybrid Warfare impacting the country's national security; and second, what countermeasures do these stakeholders propose to effectively mitigate the threats posed by 7th Generation Warfare within the broader Media Hybrid Warfare framework?

## Literature Review

7th generation warfare, popularly known as 7GW is a modern warfare theoretical concept that encompasses the use of technological innovation and practices to achieve strategic interests. Involving new weapons, tactics and classes of warfare, it has long-term implications for warfare. That's 7GW: The Application of Artificial Intelligence in Cybersecurity (Richardson, 2023). Artificial Intelligence (AI) has been very successful at identifying and responding to cyber threats as they are emerging in reality time. For example, using machine learning algorithms to evaluate enormous amounts of data may find vulnerabilities in networks (Masood & Mir, 2023).

Likewise, 7GW is a battlefield for electronic warfare-here, the Electromagnetic Spectrum (EMS) is used to disrupt or deny the enemy's communications and information systems. As Tabssum (2023) reported, 7GW will see increased use of electronic warfare as states vie for supremacy in the electromagnetic spectrum while also being very important in 7GW is space technologies. According to Ullah (2023), such as satellites and GPS satelites will be key sources of intelligence and information for tracking enemy movements or guiding guided weapons. And they also provide both communication and navigation--two crucial aspects of modern war today.

7GW, finally, has to use the drones and other unmanned systems for reconnaissance as well as assault. Rather than being limited to research and development, drones have become an increasingly prominent tool for military operations, bringing benefits such as lower costs, reduction in danger to own troops and improved flexibility of deployment. In short, 7th generation warfare is a new concept of modern technology and tactics which aim at strategic objectives (Bronnikov, 2020). Later perhaps the concept of 7GW will be extended when new technologies come along.

To any state, 7th generation warfare poses a formidable threat to national security because it enables state and non-state organizations to wage non-kinetic warfare, often surreptitiously and on feasible targets

or with tools that are hard to detect let alone defend against (Ali, 2024). One example: with social media one can wage cyber-attacks and other non-legal forms of war which, while invisible, can cause serious damage to a country's economic and investment environment, infrastructure as well as everything else likewise important in life. The new idea of "Wars for the 7th Era" describes a method to achieve strategic goals by means different from traditional warfare tactics and large-scale strategy. National Security refers to the measures taken by a country to protect against internal and external threats of its sovereignty, territorial integrity or both (Kweera, 2023).

7th Generation Warfare (7GW) presents special challenges to national security, as it presents new layers of complexity. Not only can public opinion be swayed, but critical infrastructure is also under pressure to perform better than its competitors. Does not the 7th Generation Warfare differ from earlier, traditional conflicts in that it often exploits technology and non-kinetic techniques operating within the digital realm? Rather than a 7GW/ MHW threat, presented to the General Assembly in October 2020 and other fora is seen as widespread support for its work by many governments. So exactly what is this 7GW/ MHW then? Who is responsible for defending against forces armed with knowledge that can reach anywhere and anyone, at any time? Isn't it enough to often forget the limited military value of even armed donation (Khan, 2023).

Nadeem et al. (2021) stresses that dealing with such a multifaceted threat calls for a comprehensive strategy in which defensive and offensive initiatives are both taken. This view is shared by Bris et al. (2021) who suggests that an integrated strategy involving a range of participants, substantial investment in technology and personnel, the proactive detection of signs and symptoms as well as strong bonds through coalitions would. reverse a recent trend instead. A 7GW/ MHW approach employing information and psychological operations requires evaluation beyond conventional defense models in terms of national security strategy.

Countering 7GW/ MHW requires substantial investment in cyber defense capabilities. This includes not only the purchase of advanced technologies for detecting and preventing cyber-attacks, but also a significant commitment to training and education particularly personnel capable of storing such threats in the complex, ever-changing environment (Shabbir et al., 2020). Building international partnerships to share intelligence and coordinated cyber defense initiatives is seen as vital. Fazal (2022) calls for more precaution for a country like Pakistan, which must increase its capabilities to protect critical national infrastructure from all kinds of cyber-related perils by the use advanced technology and creation highly-skilled cyber defense talent. A key aspect of this "4GW" strategy is to spread willfully false information, stirring up confusion with planted stories of fake government documents or conspiracy theories invented on social media sites like Facebook and Twitter used in conjunction with manufactured racist hatred designed to naturaly further undermine any trust in the authorities. In order to level the playing field, effective countermeasures involve work before the fact (Abd, 2022). The goal is to get information out on a timely basis and set up a modern equivalent of defusing bombs. In addition, it is also essential that cross-border disinformation campaigns be identified and neutralized through international cooperation. In addition to defensive postures, the literature suggests that active measures may be necessary, such as waging targeted network warfare. This could include cyber operations intended to disrupt adversaries' activities, break up hostile networks or achieve a " having one's own soldiers lie die " advantage in the cognitive sphere. Such operations may also be directed at particular individuals or groups threatening the state (Rana, 2020). The effectiveness of both offensive and defensive strategies in 7GW/ MHW increasingly hinges on the sophisticated application of new technologies. As far as today goes, AI has allowed us to have enough absolute advantages during wars before they even start. For instance AI can expose real-time cyber threats and responses by analyzing large data sets to find irregular patterns. AI-powered autonomic systems, such as drones, provide a reduced risk of human intervention for intelligence gathering and counteractive threats. AI also gives military commanders and staff a high level of decision support--produce new information by sifting through complex environments, derive from it something concrete for action (Boshi, 2020).

In addition to organizing principles, specific instruments of cybersecurity play an important role. These are enabling the attack of hostile targets and protecting friendly networks and communications systems against intrusion (Aslam, 2020). The provision of 5G technology brings with it major military prospects including greater bandwidth, low latency and better mobility. This will improve not only communications but also real-time command and control, autonomous vehicles including something we might not have thought much about before--the importance for seven wars soldier-mercenary wars of remote sensing capabilities (Haider et al., 2020).

The decentralized and secure nature of blockchain offers potential in safeguarding communication and transactions. Its application can make it significantly harder for adversaries to tamper with critical data or launch certain types of cyberattacks, thereby enhancing the integrity of information systems (Abbas Awan & Javaid, 2020). While still emerging, quantum computing holds transformative potential, particularly in cryptography. Its ability to break current encryption standards necessitates research into quantum-resistant algorithms. Conversely, it could enable highly secure communication channels, offering a distinct advantage in information warfare.

AR technology, by superimposing digital information onto the real world, can enhance situational awareness and decision-making for personnel, potentially in training for or responding to complex MHW scenarios. Satellites and other space-based assets play a crucial role in modern warfare, including 7GW/ MHW. They are vital for intelligence, surveillance, reconnaissance (ISR), communication, and navigation. The potential for space-based weapons, whether offensive or defensive, adds another dimension to conflict, directly impacting information dominance (Donaldson et al., 2020).

Advancements in these fields also carry implications. Nanotechnology may lead to sophisticated military materials, lightweight armor and microscopic sensors for intelligence gathering. Biotechnology could be applied to develop advanced medical treatments or more controversially, in ways that could alter human capabilities. While less direct, the intelligence and resilience aspects can feed into MHW preparedness (Bronnikov, 2020). While primarily kinetic, the development of hypersonic weapons signifies a rapidly evolving technological arms race, underscoring the shifting landscape of warfare and potentially pushing adversaries towards more asymmetric, non-kinetic MHW approaches if they cannot compete symmetrically (Muksin et al., 2023).

The rise of new technologies and capabilities such as cyber assaults, electronic warfare, space-based assets, Artificial Intelligence (AI), drones and nanotechnology has revolutionized the old paradigm of combat. To define this new type of warfare that integrates these aspects and differs greatly from traditional warfare, the phrase 7th generation warfare has been coined (Shabbir et al., 2020). The employment of technology is one of the fundamental contrasts between 7th generation combat and conventional warfare. While conventional warfare typically relies on traditional weaponry like tanks, missiles and guns, 7th generation warfare utilizes all cutting-edge technology like AI, drones and cyber-attacks (Bris et al., 2021). For example, artificial intelligence (AI) may be used to examine huge volumes of data and make real-time decisions to enhance warfare operations. Drones may conduct espionage, surveillance and reconnaissance (ISR) missions as well as perform targeted strikes against hostile targets. Cyber-attacks on enemy communication and infrastructure systems can disrupt or destroy them, hampering their capacity to fight (Rasheed & Naseer, 2021).

The character of the battlefield is another key distinction. The battlefield in 7th generation warfare is not restricted to physical settings, but may also include cyberspace, outer space and even individual human beings (Warrich et al., 2021). For example, space-based assets can provide essential information and communication capabilities, whereas nanotechnology can improve individual soldier skills and give innovative medical treatments. The usage of these new technologies also introduces new vulnerabilities that attackers and defenders might exploit. Cyber assaults may infiltrate deeply into networks and systems, interrupting

operations and stealing important data. To disrupt or degrade enemy communication networks, electronic warfare can be deployed (Ross, 2018). Artificial intelligence can be utilized to fool and influence hostile decision-making systems.

7th Generation Warfare is a considerable divergence from traditional warfare, embracing new technology and capabilities that fundamentally alter the character of the battlefield. These technologies expand so will the definition of 7th generation warfare. 7th generation warfare is based on the idea that traditional tactics and techniques are no longer viable in the modern world and new approaches must be devised to combat the emerging challenges of the twenty-first century (Khan, 2023). The goal of 7th generation warfare is to develop effective strategies, techniques and processes for coping with these new challenges. One of the key goals of 7th generation warfare is to identify strategies to fight non-state actors' employment of asymmetrical warfare techniques, such as terrorist groups, insurgent organizations and other violent extremist groups (Richardson, 2023). To get an edge over more traditional armed forces, these groups frequently employ unorthodox tactics such as propaganda, information operations and cyber-attacks. 7th generation warfare tries to create new ways of information warfare, such as the use of big data, artificial intelligence and machine learning to evaluate and respond to threats in real time, to oppose these tactics (Ullah, 2023).

Another goal of 7th generation warfare is to create successful ways to operate in urban contexts which are rapidly becoming the centerpiece of combat in the modern world. Military forces have particular obstacle in urban combat such as the need to operate in close vicinity of civilian populations while minimizing collateral damage (Hussain et al., 2023). To solve these issues, 7th generation warfare tries to create new technology and tactics that enable armed forces to operate successfully in urban contexts, such as the employment of unmanned aerial vehicles (UAVs) and other autonomous systems. In addition to these goals, 7th generation warfare explores innovative techniques to fight the danger of cyber assaults and other types of electronic warfare. This involves creating new technology for safeguarding military networks as well as new strategies for identifying and responding to cyber-attacks (Muksin et al., 2023).

Ultimately, the goal of 7th generation warfare is to remain ahead of modern warfare by developing new strategies and tactics that are successful in dealing with the growing dangers of the twenty-first century. Military forces may better adapt to the changing nature of warfare and stay one step ahead of their opponents by combining classic military tactics with modern technology and procedures.

While the existing literature provides a broad overview of the nature of 7GW/ MHW, key strategic responses and the role of various technologies, a significant portion of this discourse remains at a general or international level. There is a discernible gap in research that specifically investigates how these complex threats are perceived and operationalized against Pakistan and critically, how key Pakistani stakeholders envision and propose contextually relevant and effective countermeasures. Understanding these localized perceptions and indigenously considered solutions is crucial for developing a resilient national strategy against the multifaceted challenges posed by 7th Generation Warfare as a facet of Media Hybrid Warfare. This study aims to address this gap by exploring these critical perspectives within the Pakistani context.

## Theoretical Framework

With an example of the latter these three correlative principles Analysis Structure seems to make it possible to multiple levels 'how best way "govern to most govern well"-another world localization differentiates One 7th Generation War against Pakistan? The information technology age has brought about a seemingly unprecedented wave in modern military related terms. In Military Affairs , Revolution in Military Affairs (RMA) provides a way to understand the technological background of 7GW . As described by (Asatryan & Kalpakian, 2023) moments when new military technologies and concepts change the character and conduct of war are the moments in what we call Revolution in Military Affairs RMA. "Revolution" in the context of

7GW refers to 'a Revolution that goes beyond both left and right', driven by digital technologies, artificial intelligence and new machine-based systems shifting the focus from kinetic strikes against enemies toward information dominance. The Hybrid Warfare Doctrine provides a strategic framework for understanding how 7GW tactics operate. On the information front, cognitive domain represents a last battleground of 7GW. This theory sees that "battlespace" is not just physical anymore but also cognitive--the minds of the people as well as of soldiers, leaders and politicians alike. Its ultimate goal is to 'win the war before the war begins' through shaping perceptions, eroding trust in institutions and manipulating public discourse: thus achieve strategic paralysis without firing a shot.

## Research Methods

This research took a qualitative research method to gain more in-depth views into the perception and suggested countermeasures of 7th Generation Warfare (7GW) as one constitutive force in Media Hybrid Warfare (MHW) against Pakistan. The primary data were based on in-depth semi-structured interviews with key stakeholders within the fields of Pakistan's national security, media landscape and its cyber domain. It was chosen because, as a technique, it offers latitude in order to pursue unanticipated themes and subtle variations in perspective while still ensuring that all major research issues are thoroughly addressed by participants of an interview. Participants were selected by a purposive sampling strategy, selecting individuals from among the general categories of government and military personnel, academia, the media industry and civil society think tanks. The semi-structured interview was selected as the primary data collection method. This method provides flexibility to push emergent themes while ensuring that the core research questions are consistently addressed across all participants, producing rich and comparable data. So as to achieve the level of expertise required, 10 key experts who had significant experience on such subjects as Pakistan's national security, cyber security, media and strategic affairs were selected through a purposive sampling strategy. This was intended to ensure that the data collected would be rich and relevant, informed heavily by deep contextual knowledge. The sample included individuals from the military, government, academic types and those working in the media. Details of the participants will be provided in Table 1 below using pseudonyms in order to maintain anonymity.

**Table 1**

| Pseudonym | Area of Specialization | Institutional Affiliation (Category) | Relevant Experience (Approx. Years) |
|---|---|---|---|
| Expert 1 | National Security & Strategic Studies | Military/ Think Tank | 30+ |
| Expert 2 | Media & Propaganda Analysis | Media/ Journalist/ Analyst | 25+ |
| Expert 3 | Foreign Policy & Defense Analysis | Media/ Think Tank | 20+ |
| Expert 4 | Media & Propaganda Analysis | Media/ Journalist | 15+ |
| Expert 5 | Defense/ Public Policy Analysis | Civil Society/ Think Tank | 25+ |
| Expert 6 | Media & Propaganda Analysis | Civil Society/ Freelance Activist | 25+ |
| Expert 7 | Cyber Law and Policy | Media/ Social Activist | 25+ |
| Expert 8 | Cybersecurity & Information Technology | IT Expert | 15+ |
| Expert 9 | Cybersecurity & Information Warfare | IT Professional/ Expert | 15+ |
| Expert 10 | Cyber Law & Policy | Civil Society/ Legal | 5+ |

Data analysis was conducted using the six-phase thematic analysis framework outlined by (Braun & Clarke, 2006) , a rigorous process for identifying, analyzing, and reporting patterns (themes) within the qualitative

data. The process was conducted manually to ensure deep engagement with the participant narratives. Phase 1 involved familiarization with the data through repeated listening to interview recordings and transcribing them verbatim. In Phase 2, initial codes were systematically generated from the data while capturing salient points relevant to the research questions. In Phase 3, the codes were collated into potential themes. These initial themes were then reviewed and refined during Phase 4 and Phase 5, where they were compared against the dataset and defined, ensuring they accurately represented the data. The final step, Phase 6, involved producing this report, where the analysed themes are presented and discussed in relation to existing literature and the study's theoretical framework.

## Analysis and Discussion

The themes and sub-themes presented in this study were manually derived through careful coding and qualitative analysis of interview transcripts obtained from semi-structured interviews with 10 key experts in Pakistan. These stakeholders provided insights based on their extensive expertise in national security, media landscapes, and cyber domains.

**Table 2**

*Revised Themes and Sub-Themes Derived from Interviews*

*Part 1: Perceived Challenges of 7th Generation Warfare*

| S.No. | Themes (The Challenges) | Sub-Themes |
|---|---|---|
| 1 | The Asymmetric and Non-Kinetic Nature of the Threat | Ambiguous warfare, Deniable operations, Blurring lines between war & peace, Difficulty of attribution, Low-intensity persistent conflict |
| 2 | The Exploitation of Societal and Cognitive Vulnerabilities | Targeting societal fault lines, Disinformation & propaganda, Erosion of trust in institutions, Manipulation of public perception, Psychological operations (Psyops) |
| 3 | The Pervasiveness of Technology and Evolving Surveillance Threats | Critical infrastructure vulnerability, Cyber-attacks on key sectors, Digital surveillance risks, Weaponization of social media, Borderless digital threats |

*Part 2: Proposed Framework for Countermeasures*

| S.No. | Themes (The Countermeasures | Sub-Themes |
|---|---|---|
| 4 | Developing an Integrated National Response | Whole-of-nation approach, Coordinated messaging, Institutional coherence, Strategic communication protocols, Proactive public diplomacy, Soft power projection |
| 5 | Building Technological and Cyber Resilience | National cybersecurity shield, Critical infrastructure protection, Enhancing ISR capabilities, Early warning systems, Developing indigenous space & cyber technology |
| 6 | Fostering Cognitive Resilience and Public Awareness | National narrative building, Media & digital literacy education, Independent fact-checking initiatives, Public awareness campaigns, Promoting critical thinking |

The analysis of the semi-structured interviews with 10 key experts revealed several key themes related to the threats of and countermeasures against 7th Generation Warfare (7GW) in Pakistan. To directly address the study's research questions, these findings are presented in two main sections. The first section explores the specific challenges of 7GW as perceived by stakeholders, answering the question of how this new form of conflict impacts Pakistan's security. The second section outlines the strategic countermeasures proposed by these experts, addressing the question of how Pakistan can effectively mitigate these threats.

### Part 1: The Perceived Challenges of 7th Generation Warfare

This section details the primary challenges of 7GW identified by Pakistani stakeholders, framing the threat as a complex, multi-layered phenomenon that targets the very fabric of the state and society.

#### 1. The Asymmetric and Non-Kinetic Nature of the Threat

A primary challenge identified by participants is the fundamentally asymmetric and non-kinetic character of 7GW, which blurs the lines between war and peace and complicated traditional defense planning. This perception aligns with the Hybrid Warfare Doctrine, which describes the use of ambiguous, deniable, and low-intensity actions to achieve strategic goals without triggering a conventional military response. Experts noted that hostile actors, both state and non-state, leverage this ambiguity to engage in persistent, low-level conflict through cyber-attacks and information campaigns. For Pakistan, a significant challenge lies in attribution; it is often difficult to definitively prove the source of a disinformation campaign or a cyber-attack on critical infrastructure, making a proportional response nearly impossible. This creates a strategic paralysis where the nation is under constant attack, yet the aggression remains below the threshold that would justify a conventional military retaliation.

#### 2. The Exploitation of Societal and Cognitive Vulnerabilities

Experts consistently highlighted that 7GW's most potent threat is its deliberate exploitation of Pakistan's internal societal, political, and ethnic fault lines. This finding is best understood through the lens of Information Warfare and the Cognitive Domain Theory, which posits that the modern battlefield has shifted from the physical to the psychological, targeting the perceptions, beliefs, and decision-making processes of a population. Participants expressed concern that hostile narratives are specifically engineered to sow distrust in state institutions like the military and judiciary, amplify political polarization, and fuel secessionist sentiments in regions like Balochistan. These campaigns are not random acts but are methodical psychological operations (psyops) aimed at eroding national cohesion and the public's will to resist. As one expert warned, the goal is to "make society defeat itself," a clear articulation of a cognitive-centric strategy that seeks to achieve victory by creating internal chaos rather than by external force.

#### 3. The Pervasiveness of Technology and Evolving Surveillance Threats

The third major challenge stems from the technological underpinnings of 7GW, which represents a new Revolution in Military Affairs (RMA) driven by digital hyper-connectivity. Participants identified a dual threat: the vulnerability of Pakistan's critical national infrastructure to cyber-attacks and the pervasive risk of digital surveillance targeting both government officials and ordinary citizens. Experts pointed to incidents such as attacks on the banking sector and the national power grid as tangible examples of how non-kinetic means can have devastating physical and economic consequences. Furthermore, the proliferation of social media and insecure communication platforms creates a vast surface for hostile intelligence agencies to monitor public sentiment, identify influential voices, and disseminate propaganda with pinpoint accuracy. This technological pervasiveness means the state is no longer defending fixed borders but a fluid, borderless digital domain where every citizen with a smartphone is a potential target or vector for a threat.

## Part 2: A Proposed Framework for Countermeasures

In response to these challenges, stakeholders proposed countermeasures of a multi-faceted nature, all designed to build up national resilience: It answers this new road to peace for a changing world. This framework goes beyond the conventional defense paradigms and calls for both hybrid and cognitive nature challenges of threat.

#### 1. Developing an Integrated National Response

To oppose the cohesive strategy of hybrid actors, meeting participants all believed that the whole nation should take united action synchronizing efforts by various elements of state power. This "whole-of-nation"

approach requires breaking the walls between military, government, and non-governmental sectors, creating what is known in literature as "strategic communication." This is not a set of one-size-fits-all countermeasures. Rather, it is designed according to the specific nature and degree of challenge neighboring countries face from their particular neighbors. The recommended countermeasures include setting up a central organ to coordinate national policy targets in matters like culture and education, launching active public diplomacy campaigns aimed at shaping global public opinion and obtaining new strength for the international discourse, and using Pakistan's cultural and diaspora assets for soft power. This sort of plan is intended to establish institutional unity and present a united front, so as deny the organized opponents they seek another opportunity.

### 2. Building Technological and Cyber Resilience

Facing the technological challenges of 7GW, experts propose a comprehensive plan of technological security and technological innovation that matches a straightforward application of RMA principles. As core elements in this tilter formula, significant funds will be put into national security infrastructure, including improving the National Response Center for Cyber Crimes (NR3C) and developing sovereign capability for defense of threat to critical infrastructure. Participants also stressed the imperative of achieving full-fledged space capability, but this is not for armament. Rather, it is so that we can make secure communications and enhanced Intelligence, Surveillance, and Reconnaissance (ISR) to pick up hybrid threats when they are still even 'virtual big rumblings.' This forward-leaning technological posture is regarded as essential for regaining sovereignty in the digital and space realms.

### 3. Fostering Cognitive Resilience and Public Awareness

One of the most important countermeasures adopted was the suggestion that Pakistanis should start to arm themselves with rational thinking. It's an idea that seeks to "vaccinate" the mind over the long term rather than use short-term controls. Among proposed solutions, making media literacy compulsory course material for all students and schools was viewed as particularly important, because it would enable the public at large to develop a critical capacity and insist on high-quality sources of information. Experts also called for the establishment of a fact-checking body independent and reputable, in addition to campaigns by the government or social justice organizations for public awareness exposing its most common tactics disinformation. This countermeasure aims to turn Chinese people into something like a "Resource" for the country by themselves growing their mental prowess. This will enable them with newly gained shrewdness to prevent and turn against hostile narratives even before they reach ultimate form, thus fortifying both nation and individuals from within.

### Countering Propaganda by Defending the Cognitive Domain

A central theme emerging from the interviews was the urgent need for a proactive and sophisticated strategy to counter hostile propaganda. Participants stressed that reactive, defensive measures are no longer sufficient. This finding is best understood through the lens of Information Warfare/Cognitive Domain Theory, which posits that the primary objective of 7GW is to shape perceptions, erode public trust, and fragment societal cohesion, effectively winning the conflict in the minds of the population before any physical battle.

The strategic importance of this is starkly illustrated by real-world examples, such as the long-running disinformation campaign against Pakistan exposed by the EU DisinfoLab. This operation utilized hundreds of fake media outlets and resurrected defunct NGOs to target international institutions and manipulate global opinion, a clear attempt to isolate Pakistan diplomatically and attack its cognitive domain on a global scale. The experts' call for a "comprehensive propaganda strategy is a direct response to such threats.

This aligns with academic literature, where scholars like (Warrich et al., 2021) and (Imran & Zafar, 2021)argue that hybrid threats deliberately target a nation's societal fault lines. The countermeasures proposed by the interviewees such as investing in national narrative building and enhancing media literacy are not just public relations exercises; they are fundamental components of national defense aimed at building what experts term "cognitive resilience" against information attacks.

## Conclusion & Recommendations

7th GW is a new and emerging form of warfare that differs greatly from traditional warfare. Its goals include using technology and unchivalrous manners to win public opinion over to boost an antidemocratic country's leaders and manipulate the media. Thanks to the use of modern technology tools such as cyber-attacks, artificial intelligence, and social media platforms, Seventh Generation Warfare is even more effective and devastating. If Pakistan is to effectively combat 7th GW and safeguard its political independence and territorial sovereignty, it must develop an integrated propaganda offensive. This should involve traditional and even new social media in providing accurate information which the public will find believable. The authorities must set up a special agency to monitor public disinformation and coordinated efforts aimed at refuting it. Pakistan must also protect critical infrastructure and communications networks from cyber attacks.

The government needs to develop a National Cyber Security Policy and establish a National Cyber Security Coordination Secretariat to coordinate efforts against information war. Pakistan also needs to beef up its intelligence gathering and analysis capabilities in order to identify and nip in the bud 7th GW terrorism or extremism. In addition, Pakistan must strengthen border security in order to prevent people and goods from moving across its international boundaries without interference. The government must implement biometric screening measures and other technologies to enhance border security, and try to improve cooperation with other countries in tackling cross-national security issues. Most importantly, Pakistan must work hard to build public trust and support for its efforts to fight 7th GW. This may involve getting civil society groups, private sector organizations and founds together to develop more effective communications strategies; increasing transparency, handling activities in a lawful and legitimate way; and publishing regular updates on progress made in these areas. In conclusion, effectively combating 7th GW is a matter of great concern to Pakistan, and by implementing the above strategies Pakistan can succeed in effectively combating 7th GW and securing long-term security and stability.

## Recommendations

It is necessary for the Government of Pakistan to establish a central National Counter-Hybrid Warfare Cell, which will enable comprehensive policy and rapid response by all functional departments. Provision of resources should focus on creating a strong National Cybersecurity Shield, which aims to protect vital infrastructure as well as on the introduction of compulsory digital literacy courses within the national education system. These measures are essential to mount an integrated defense against the cognitive and technological components of 7GW

## Limitations of the Study

The findings of this study derive from a qualitative analysis of ten experts purposively selected and hence cannot be taken as statistically representative ofthe population at large. The level of sensitivity surrounding the national security topic might also have affected how in-depth participants were prepared to go. Future research which is more quantitative in nature might seek to confirm these findings across a wider spectrum of society and to compare what Pakistan has known of hybrid threats with the experience other nations have had.

## References


Awan, A., & Javaid, F. (2020). Space Militarization Race among China-Russia and USA: Implications for South Asia. *Asian Studies A Research Journal of South Asian Studies*, *87*(1).

Abd, S. Al. (2022). SOCIAL MEDIA AS A THREAT TO NATIONAL SECURITY: A CASE STUDY OF TWITTER IN PAKISTAN. *Margalla Papers, 26*(2). https://doi.org/10.54690/margallapapers.26.2.117

Ali, M. (2024). 'Satrah Din, Satrah Saal': Media, Propaganda and Virtual Warfare in the India-Pakistan War of 1965. *South Asia: Journal of South Asia Studies, 47*(2). https://doi.org/10.1080/00856401.2023.2262288

Asatryan, G., & Kalpakian, J. (2023). The Palgrave handbook of national security. *Intelligence and National Security, 38*(2). https://doi.org/10.1080/02684527.2022.2031664

Aslam, S. (2020). Hybrid warfare and social media: need and scope of digital literacy. *Indian Journal of Science and Technology, 13*(12). https://doi.org/10.17485/ijst/v13i12.43

Baber, I. (2020). *Pakistan being subjected to 5th-generation warfare in "massive way" but we are aware of threats: DG ISPR – Pakistan.* Dawn.Com. Daily Dawn Newspaper, 5.

Boshi, R. (2020). LATENT IMAGES ON THE CAMERA'S WALL: Forensic aesthetics as photography. *Photographies, 13*(2). https://doi.org/10.1080/17540763.2020.1733642

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2). https://doi.org/10.1191/1478088706qp063oa

Bris, A., Wang, T. Y. H., Zatzick, C. D., Miller, D. J. P., Fern, M. J., Cardinal, L. B., Gregoire, D. A., Shepherd, D. A., Westphal, J. D., Shani, G., Troster, C., Van Quaquebeke, N., Lanaj, K., Hollenbeck, J. R., Ilgen, D. R., Barnes, C. M., Harmon, S. J., Feldman, E. R., DesJardine, M. R., … Sangiorgi, F. (2021). KNIGHTS, RAIDERS, AND TARGETS - THE IMPACT OF THE HOSTILE TAKEOVER - COFFEE,JC, LOWENSTEIN,L, ROSEACKERMAN,S. *JOURNAL OF BANKING & FINANCE, 37*(1).

Bronnikov, I. A. (2020). Self-organization of Citizens in the Age of Digital Communications. *Outlines of Global Transformations: Politics, Economics, Law, 13*(2). https://doi.org/10.23932/2542-0240-2020-13-2-14

Donaldson, L. J., Rockville, W., Sorra, J., Gray, L., Streagle, S., Famolaro, T., Yount, N., Behme, J., Surugue, J., Vulto, A., Health Service Executive, Rafter, N., Hickey, A., Conroy, R. M., Condell, S., O'Connor, P., Vaughan, D., Walsh, G., Williams, D. J., … Lalor, D. J. (2020). Critical Appraisal Checklist. *Expert Opinion on Pharmacotherapy, 11*(1).

Fazal, M. S. (2022). India's Hybrid Warfare Strategy towards Pakistan in the Backdrop of Social Media (2018-2022). *Annals of Human and Social Sciences, 3*(II). https://doi.org/10.35484/ahss.2022(3-ii)80

Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science, 12*(1). https://doi.org/10.1140/epjds/s13688-023-00414-5

Haider, M. W., Azad, T. M., & Warrich, H. U. R. (2020). A Critical Review of Hybrid Warfare: Challenges to Pakistan. *Global Mass Communication Review, V*(IV). https://doi.org/10.31703/gmcr.2020(v-iv).06

Hussain, S., Roofi, Y., Faheem, F., Qamar, M. T. R., & Ajmal, S. (2023). Role of Media in Hybrid Warfare in Pakistan: How to Convert Challenges into Opportunities. *Journal of South Asian Studies, 11*(3). https://doi.org/10.33687/jsas.011.03.4693

Imran, S., & Zafar, M. A. (2021). Propaganda Warfare: Indian Disinformation Campaign against Pakistan. *Global Strategic & Securities Studies Review, VI*(II). https://doi.org/10.31703/gsssr.2021(vi-ii).04

Khan, S. (2023). Leaving Comrades to Die: Shahadat, Soldiering and Accidental Death on the Siachen Glacier. *South Asia: Journal of South Asia Studies, 46*(2). https://doi.org/10.1080/00856401.2023.2180897

Kweera, R. (2023). Drones in Modern Warfare: Utilization in India-Pakistan Cross-Border Terrorism and Security Implications. *Strategic Analysis, 47*(4). https://doi.org/10.1080/09700161.2023.2288989

Masood, M. D., & Mir, A. (2023). Role of Social Media in Securitization of Baloch Conflict. *Progressive Research Journal of Arts & Humanities (PRJAH), 5*(1). https://doi.org/10.51872/prjah.vol5.iss1.230

Matloob, N., Matloob, N., & Ishaq, S. (2023). Hybrid Warfare: Strategies and Counterstrategies in the India-Pakistan Rivalry. *Journal of Peace and Diplomacy, 4*(1). https://doi.org/10.59111/jpd.004.01.043

Muhammad Usman, Dr. S. (2024). Pakistan in the Crosshairs and the Rising Stakes of Strategic Information Warfare. *Journal of Research in Social Sciences, 12*(1). https://doi.org/10.52015/jrss.12i1.235

Muksin, N. N., Sinaga, A. B., Hidayat, H., Handoko, D., & Shabana, A. (2023). Ganjar Pranowo's Storytelling and Political Image on Social Media. *KOMUNIKA: Jurnal Dakwah dan Komunikasi*, *17*(2), 175-190. https://doi.org/10.24090.komunika.v17i2.7206

Nadeem, M., Mustafa, G., & Kakar, A. (2021). Fifth Generation Warfare and its Challenges to Pakistan. *Pakistan Journal of International Affairs, 4*(1).

Nadvi, M. J., & Nadwi, M. K. (2022). Understanding the Cohesion and Stability Issues of Pakistan: Appraisal & Solution. *Al-Wifaq, 5.2*. https://doi.org/10.55603/alwifaq.v5i2.e1

Ogden, M. (2020). Killer apps: war, media, machine. *Critical Studies in Media Communication, 37*(5). https://doi.org/10.1080/15295036.2020.1814118

Rana, J. (2020). Introduction. Migrants in a Neoliberal World. In Terrifying Muslims. https://doi.org/10.1515/9780822393665-002

Rasheed, M. R., & Naseer, M. (2021). Digital Disinformation & Domestic Disturbance: Hostile Cyber-Enabled Information Operations to Exploit Domestic Issues on Twitter. *IPRI Journal, 21*(02). https://doi.org/10.31945/iprij.210204

Richardson, M. (2023). Drone trauma: violent mediation and remote warfare. *Media, Culture and Society, 45*(1). https://doi.org/10.1177/01634437221122257

Ross, R. S. (2018). Nationalism, Geopolitics and Naval Expansionism From the Nineteenth Century to the Rise of China. *Naval War College Review, 71*(4).

Shabbir, T., Farooqui, Y. S., Waheed, S., Usman, S., & Memon, A. A. (2020). 'Open Data'Technology and Fifth Generation Warfare (A Pakistan Perspective). *Ilkogretim Online*, *19*(4), 5183-5192. https://doi.org/10.17051/ilkonline.2020.04.764927

Sultana, I., Mahmood, R. S., & Ahmed, H. Y. (2021). Pakistani Print Media as Political Propaganda Tool: A Study of Panama Issue. *Global Political Review, VI*(II). https://doi.org/10.31703/gpr.2021(vi-ii).10

Tabssum, S. (2023). Interpretive Structural Model (ISM) based Analysis of Issues of National Integration in Pakistan: A Case Study of Balochistan. *PAKISTAN LANGUAGES AND HUMANITIES REVIEW, 7*(II). https://doi.org/10.47205/plhr.2023(7-ii)42

Ullah, U. (2023). Perception of Fifth Generation Warfare Among Social Media Users: A Case of Punjab University Students. *Journal of Social & Organizational Matters, 2*(1). https://doi.org/10.56976/jsom.v2i1.19

Warrich, H. U. R., Haider, M. W., & Azad, T. M. (2021). Media as an Instrument of Hybrid Warfare: A Case Study of Pakistan. *Global Mass Communication Review, VI*(I). https://doi.org/10.31703/gmcr.2021(vi-i).02