

DECODING SIXTH-GENERATION WARFARE IN SOUTH ASIA: LESSONS FROM THE 2025 INDIA-PAKISTAN WAR

Dr. Zainab Murtaza^{*1}, Hira Arshid², Dr. Anwar Ali³, Dr. Khadija Murtaza⁴

^{*1}Visiting Assistant Professor, Department of Political Science, Government College University Faisalabad

²Visiting Lecturer, Department of Political Science, Government College University Faisalabad

³Assistant Professor (OPS), Department of Political Science, Government College University Faisalabad

⁴PhD, Political Science, Government College University Faisalabad

¹zainabmurtaza545@gmail.com, ³anwarali@gcuf.edu.pk, khadijamurtaza12@yahoo.com⁴

Corresponding Author: *

Dr. Zainab Murtaza

DOI: <https://doi.org/10.5281/zenodo.18181527>

Received
30 October 2025

Accepted
14 December 2025

Published
28 December 2025

ABSTRACT

The technological advances of the 21st century have expanded traditional concepts of war and security. This advancement transforms the concept of war and security that includes a significant element of artificial intelligence or autonomous technologies and systems. It is now considered to be one of six operational domains for warfare, the remaining five being land, sea, air, space, and cyberspace. This new realm of confrontation has encouraged states globally to preserve and develop offensive or defensive warfighting capabilities according to their capabilities. The recent four-day war between Pakistan and India exemplifies Sixth Generation Warfare (6GW) with its use of non-contact operations, precision strikes, and electronic warfare (EW). This research analyses the Indo-Pak conflict through the lens of Six Generation Warfare. Through the application of realist and constructivist theories of political science, this article examines how the advanced technologies and strategies of 6GW reshape state behaviour, power dynamics, and regional stability in South Asia.

Key Words: Pakistan, India, Six Generation Warfare, Cyber Warfare, Electronic Warfare

Introduction

Warfare has changed tremendously throughout the ages, from hard battle lines to blurry digital frontlines. Each generation of warfare signifies a major transformation in the methods of conducting battles, influenced by developments in technology and tactical approaches. However, the evolution of warfare not only reflects changes in military strategy but also impacts global politics and civilian life. War is always a failure of humanity, it is a collective failure of values. Since the three main characteristics of foreign policy are values, interest and power, you only achieve your interest and gain power but lose values with the technique of war. Memory is a weapon in the war of narrative. We are entering an era where the economy is your security, technology/cyberspace is your territory, and AI is

your army. As nations adapt to these transformations, the ethical implications of modern conflicts continue to provoke intense debate among scholars and policymakers alike. In the past, early industrial wars were smoke-filled trenches and now the quiet algorithms of AI-powered psychological manipulation. But knowing these periods reveals not only how wars are won but how they are fought without firing a single shot.

Sixth Generation Warfare (6GW) is a paradigm shift in military strategy that goes beyond traditional kinetic operations to utilize artificial intelligence (AI), autonomous systems, cyber capabilities, and information supremacy. This evolution reflects a shift towards a more holistic approach, where the battlefield extends into the digital realm and public perception is as important as physical dominance. As

states adapt to these new realities, the integration of technology and psychological operations will likely become central to achieving strategic objectives. The article describes 6GW as a dramatic shift marked by precision, data-driven tactics, and the use of cognitive capabilities to achieve strategic goals without large-scale physical battles. The 2025 India-Pakistan conflict, which began with a terrorist assault in Pahalgam on April 22, 2025, and escalated through India's Operation Sindoor and Pakistan's

Operation Bunyan-un-Marsoos, is a real-world example. Both states's operations demonstrated counter-narrative strategies and precision strikes. The conflict underscores the risks of escalation in nuclear-armed states. This study examines the dispute how 6GW affects state behaviour, narrative control, and escalatory dynamics. However, as night follows days, warfare has changed, from muskets to machine learning.

Warfare Gen	Dominant Factor
1GW	Massed formations and manpower
2GW	Firepower and attrition
3GW	Speed and maneuver
4GW	Asymmetry and ideology
5GW	Cyber and info dominance
6GW	AI, autonomy, perception & psychological control

Sixth-generation warfare (6GW) is a theoretical concept in the evolution of military conflict that builds on previous generations by combining artificial intelligence, robotics, cyber, information dominance, and non-kinetic tools (such as psychological warfare and economic manipulation) to achieve strategic goals without traditional large-scale military war. Sixth-generation warfare (6GW) covers the control of information, the utilisation of sophisticated technology, advanced military theory and the indirect manipulation of an adversary's society, politics, economics, and perceptions. This approach indicates a transformation in the exertion of power and the resolution of conflicts, prioritizing strategy, psychological operations and precision rather than brute force (Ali, 2025). It's also known as cognitive warfare, in which winning the narrative is more important than retaining land. This paradigm is closely related to the 2025 India-Pakistan confrontation, in which both countries used sophisticated technology to conduct standoff operations under a nuclear umbrella.

Sixth-Generation Warfare Features:

There are the features of six generation warfare with examples

Drones and unmanned systems

The unmanned system is used for quick and secret act by approaching 'fire and forget'. It can be exemplified by Israel's Harpy and Harop (Loitering Munitions). These are drone systems that can patrol a certain region autonomously, detect radar emissions, and engage hostile radars without the need for human interaction (Israel Aerospace Industries HAROP loitering munition, 2023). They're basically AI-guided kamikaze drones.

Cyber tactics:

Cyberspace has changed the way we think about war. The cost of conducting offensive cyber operations is much lower than on the physical battlefield. As a result, states are increasingly relying on digital strategies, where espionage and sabotage can occur without the traditional consequences of war. However, this shift not only alters military strategies

but also raises ethical questions about the limits of conflict in an interconnected world. In 2009, Stuxnet targeted Iranian nuclear centrifuges and caused physical damage by altering their speed (Fildes, 2010). It is one of the earliest documented instances of cyber weapons wreaking havoc in the real world. While, in 2021, Dark-Side ransomware assault, forced a major US petroleum pipeline to shut down and affected its fuel delivery throughout the East Coast (Lakshmanan, 2021). Though, cutting-edge technology is essential to improving cybersecurity, but it doesn't always make states less vulnerable to cyberattacks.

Psychological manipulation

Sometimes social media is used to manipulate population to cause unrest or political shifts. Arab Spring is the best example of it. Where protests were planned via social media, Facebook or Twitter, encouraging civilians to stand up against authorities in the Middle East. Furthermore, Though, Cyber media may be used to demoralise communities during times of active warfare. Just like happened in 2022, a fake video of Zelensky instructing Ukrainian troops to surrender was disseminated online (Allyn, 2022). While, in 2023, a deep fake image described an explosion near the Pentagon temporarily circulated on social media and triggered a momentary drop in the stock market (Haddad, 2023).

Quantum & Space Technologies

States are using technology for communication, surveillance, and disruption. China launched the world's first quantum communication satellite named Micius in 2016 to test ultra-secure quantum key distribution (QKD), aiming for unhackable global communications. A first step towards quantum military capabilities which shows that the world is poised to begin an era of quantum telecommunications research (Ding, 2016). In contrast, Global Positioning System (GPS) signals have evolved as an indispensable element of modern warfare, with electronic warfare (EW) playing a critical role in the process of disrupting or manipulating these signals, as occurred in the conflict between Pakistan and India in 2025. Imagine trying to listen to your favorite radio station when someone is blaring loudly on the same

frequency, making it difficult to hear the music. That's exactly what GPS jamming achieves. It overwhelms the signal, preventing devices from getting a clear readout. However, there is an even more stealthy method called "spoofing," in which fake GPS signals are generated to confuse devices, perhaps throwing them off track. It highlights the dangers of relying solely on GPS and the need for alternative navigation sources to ensure accuracy and security (Burkey, 2025).

Research Methodology

This paper employs a qualitative case study technique to examine the India-Pakistan conflict framework through the prism of six-generation warfare. To better comprehend the India-Pakistan war, this study uses a combination of primary and secondary materials. The research investigates the escalation of the war, military reactions, political narratives, and diplomatic endeavors via the analysis of documents, press announcements, books, articles, and media coverage. However, this study employs a descriptive, exploratory, and analytical technique to investigate the Pakistan-India four-day conflict through the prism of six-generation warfare. In addition, the study intends to get a comprehensive understanding of the impact of the conflicts on the security of the region, as well as the fragile relationship that exists between India and Pakistan.

Power and Deterrence

According to Realists, conflict as a struggle for power in a chaotic system. 6GW's precision and data-driven strategy or autonomous system like drones enhance the state's ability to project power without triggering catastrophic surges. This new realm of confrontation has encouraged states globally to secure and build offensive or defensive warfare capabilities as per their potential (Ashraf, 2025). India's Operation Sindoor, by targeting symbolically important locations like Muridke, challenged Pakistan's nuclear deterrence. India signaled that technological superiority could bypass conventional barriers. Meanwhile, Pakistan's response is using AI-powered drones and EW to counter India's conventional edge and maintain a balance of power, maintain deterrence again. However, Pakistan got the competitive advantage through use of swarm warfare and EW technology to disrupt India's

command structure. In result that precise and strategic planning created a “fog of war” that limits India’s operational momentum. However, the nuclear shadow, as Samson-Simon Shroff has argued, complicates 6GW by introducing new forms of coercion, where states coerce without any handicap. The rapid decline in conflict suggests that the precision of 6GW creates increasing buffers, but the compressed geography of South Asia increases the risks of miscalculation.

Constructivism

While, Constructivists focuses on identities and narratives. Though, India started Operation Sindhoor after pahalgam incident and tried to reinforce its identity as a powerful state. Pakistan countered by portraying India's actions as unprovoked. Social media platforms amplified these narratives, with both sides using data-driven analytics to target audiences. However, 6GW manipulates perceptions to influence decision-making and infiltrates the adversary’s “observe, orient, decide, act” (OODA) loop. Pakistan’s use of Chinese satellite imagery and AI to develop a counter-narrative is perfect example of this. Further, OODA by Pakistan challenged India’s narrative of regional dominance. The four-day duration of the 2025 conflict and the lack of large-scale military engagements support this. However, they were Pakistani who hit the lights of Indian military posts and played the anthems on Indian channels. As both states used 6GW to achieve strategic goals without crossing nuclear thresholds. However, the speed of AI-powered operations shortens decision-making timelines, can increase the risks of miscalculation in a nuclear context.

Warfare from Line Formations to Cyber-fronts

Periodic crises between Pakistan and India, somehow, became the cause of the 4-day war of May 2025. On April 22, 2025, 26 Indian citizens, most of them tourists, were killed in a deadly militant attack in Pahalgam, Indian-administered Kashmir. India has blamed Pakistan-based terrorist groups for the attack (Mogul, Iyer, & Saifi, 2025). Though, Pakistan has denied the Indian allegation. Further, Pakistan has promised a transparent investigation, assuring the team or cooperation. On April 23, India sealed the border crossings. The next day,

however, Pakistan closed its airspace and suspended trade ‘with immediate effect’ (Shahzad, Shahid, & Bukhari, 2025). India launched Operation Sindhur, firing missiles towards Pakistan, saying it was in retaliation for the attack on Pahalgam.

Pakistan Strongly Condemns India’s Blatant Aggression, said by Pakistan’s ministry of Foreign Affairs. Furthermore, it added in an unprovoked and blatant act of war, the Indian Air Force, while remaining within Indian airspace, has violated Pakistan’s sovereignty using standoff weapons, targeting civilian population across international border in Muridke, Sialkot and Bahawalpur, and across Line of Control in Kotli and Muzaffarabad, Azad Jammu and Kashmir. India’s act of aggression has resulted in martyrdom of civilians, including women and children. This act of aggression has also caused grave threat to commercial air traffic. We strongly condemn India’s cowardly action, which is a flagrant violation of the UN Charter, international law, and established norms of inter-state relations (Affairs, 2025).

Pakistan responded with its own action, resulting in intense fighting between them, by using drones, air strikes, cross-border firing and cyber strikes. Though, a ceasefire was reached after four days by international mediation. However, it was the war that fought between them without crossing borders. However, Pakistan has demonstrated its expertise in sixth-generation warfare, a modern military doctrine that emphasizes precision, deception, and psychological disruption. In response to India's aggressive actions, including missile attacks on Pakistani air force installations, Pakistan has refrained from escalation, defending its sovereignty. Furthermore, this doctrine focuses on achieving strategic objectives through targeted operations, economic disruption, and political destabilization of the adversary rather than territorial conquest. When India launched unprovoked missile attacks on Pakistani air bases, Pakistan exercised its right to self-defense under Article 51 of the United Nations Charter. According to the DG ISPR, the targets include Suratgarh, Sirsa, Adampur, Bhuj, Nalia, Bathinda, Barnala, Harwara, Awantipora, Srinagar, Jammu, Mamoon, Ambala, Adampur and Pathankot, where significant damage was sustained to air force and aviation bases (team, 2025).

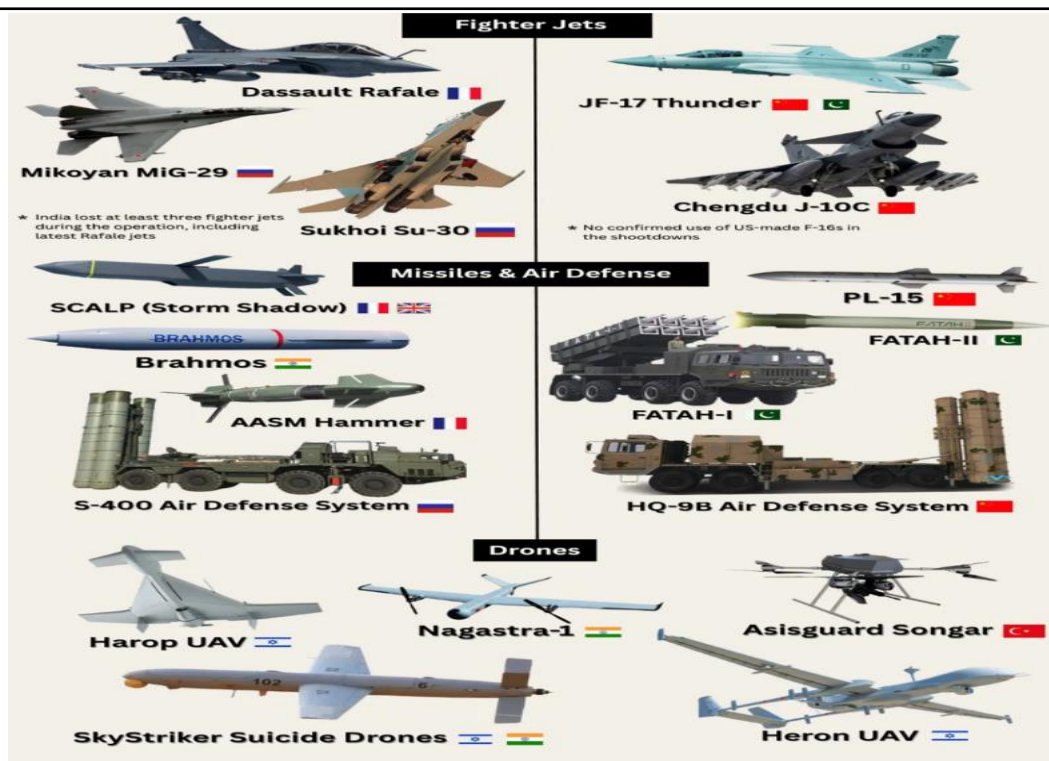
Following the Pahalgam terror assault, both India and Pakistan, barred each other's planes from accessing their airspace. The limitations apply to both commercial and military aircraft registered or operated in the two nations. Flight times have increased by an average of sixty to ninety minutes on routes that connect India to Europe and the United States. These routes have been experiencing the greatest impact. The blockade of Pakistani airspace results in a loss of ₹4,000 crore for Air India. The airspace closure has resulted in longer flight times and higher fuel and crew costs, affecting Air India's busiest routes to Europe and North America (Desk, 2025). However, this is proof that 6GW is a silent storm, blinding the enemy.

Though, the Pakistani Air Force's response was accurate and effective, neutralizing the incoming threats and shooting down an Indian Rafale fighter jet. Meanwhile, India's exaggerated claims of attacking Pakistani cities and destroying airbases have been refuted under international scrutiny. Nevertheless, Pakistan's digital counter-offensive broke India's information blockade. Pakistan used a tactic whereby after shutting down Indian YouTube channels, its patriotic songs were broadcast on Indian YouTube channels, which upset India. A nationalist military anthem on Indian YouTube has sparked widespread attention and concern among Indian users, demonstrating the power of targeted digital communication. Pakistan's federal minister said that Pakistan used digital warfare tools to enhance the morale of its people (APP, 2025). Pakistan's win can be attributed to its mastery of sixth-generation warfare, which emphasizes non-contact, high-precision operations, psychological effects, and information dominance. In short, this strategic doctrine aims to disrupt an enemy's economy, destabilize their political objectives, and damage their global reputation without resorting to

all-out war. Unlike traditional frontlines, 6GW/network-centric/hybrid conflicts, are characterized by their hidden and ongoing nature, targeting civilizations through drones, propaganda, and hacking.

Military domain

The 2025 India-Pakistan conflict showcased cutting-edge technology from both sides. India's Brahmos missile and French SCALP penetrated Pakistani defenses, While Pakistan's Chinese J-10 jets and HQ-9 system shot down five Indian aircraft, including three Rafale jets and one each of a Russian aircraft, a Su-30 and a MiG-29 (Jaspal, 2025). Pakistan's Air Chief Marshal Zaheer Sidhu targeted India's prized Rafale fighter jets, and shot down it which shocked the international military community. The downing of Rafale was due to a failure of Indian intelligence regarding the range of the PL-15 missile. Pakistan's electronic warfare attack, which was aimed at confusing the Indian pilots, was tactically successful. The battle involved 110 aircraft, making it one of the largest air battles in decades. Pakistan's "kill chain" network is linked to air, ground and space sensors, providing improved situational awareness. This network included Data Link 17, which connected Chinese hardware to Swedish surveillance aircraft. Electronic warfare refers to the use of electromagnetic energy to disrupt or deceive enemy systems, often to gain a tactical advantage. Pakistan's use of electronic warfare was important part of its strategy to defeat Indian forces (Shah & Patel, 2025). Pakistan used the Turkish Bayraktar drone in the first drone war between nuclear-armed countries. The Bayraktar TB2 is not the only Turkish drone model in Pakistan's arsenal (Andreopoulos, 2025), and India deployed Israeli Heron UAVs for surveillance and attacks (Biswas, 2025).



Source: (Reports, 2025)

Cyber attacks

Pakistan allegedly attacked Indian power grids and official websites which led to significant disruptions in several Indian domains, including electrical infrastructure and petroleum systems. According to sources, the Pakistani cyber team caused considerable damage to Indian communications by disabling official government emails and OTP infrastructure, as well as severely disrupting national communications (Team T. , 2025).

According to reports, the official website of the BJP has been hacked. Further, the hacked websites include the Crime Research Investigation Agency, Mahanagar Telecommunication Company Limited, Bharat Earth Movers Limited, and the All India Naval Technical Supervisory Staff Association. The hacked websites, including those of Hindustan Aeronautics Limited and Border Security Forces, and the data of the Unique Identification Authority of India have been compromised. The leaked data also includes information from the Indian Air Force, Maharashtra Election Commission and other sources. Additionally, around 2,500 surveillance cameras have been compromised (Mansoor, 2025).

A Pakistani cyberattack team has attacked the Maharashtra State Electricity Transmission Company Limited, causing a complete power outage. The attack has wiped the records of all commercial and domestic meters in the state of Maharashtra (Team R. P., 2025).

Pakistani hackers managed to deface some web pages and create online noise, but caused negligible lasting damage to India's critical assets. Hackers linked to India also retaliated against Pakistan, taking down or defacing Pakistani websites in tit-for-tat moves. The attacks featured elements of sophisticated cyber warfare, including GPS spoofing and targeted intrusions into Indian defense networks. Despite the scale of the cyberattacks, most Indian government and critical systems withstood the attack or were quickly restored. India's cybersecurity professionals worked around the clock to apply security patches and monitor networks. The attackers had an "abysmal success rate" of 0.01%. Indian cyber authorities are engaged in counter-attacks, probing Pakistani networks and conducting selective operations (Baek, 2025).

Propaganda Warfare

Perception management is categorized as an important part of the propaganda warfare strategy. Perception management influence the enemy's decision-making hierarchy and the general public. The 2025 India-Pakistan conflict showcased sixth-generation warfare, with psyops and disinformation campaigns dominating the narrative. as stated by Clausewitz, the fog of uncertainty has been a fundamental property of military action, as cyber domain did so in four-day war between Pakistan and India. While disinformation or propaganda tactics added the fog of military action and keep the enemy unaware of real intentions.

During a tense period in India-Pakistan relations, Indian mainstream media was criticized for spreading fake news, doctored visuals, and sensationalist coverage, driving public anxiety and misinformation. Many TV channels aired misleading footage, including clips from conflicts in Gaza and Lebanon, falsely claiming they showed Indian strikes on Pakistani cities. Channels also reported fabricated stories, such as a coup in Pakistan, attacks on Islamabad, and Indian military victories. The use of fake news and dramatic visuals, including war room sets and air raid sirens, sparked backlash online, with critics calling it a national embarrassment that undermined journalistic integrity.

Indian news channels transformed their studios into war rooms to create a war-like atmosphere, with airstrike sirens, helicopters and jets flying in the background, and maps of Pakistan on target. They used doctored visuals, video games, and AI-generated footage, criticizing online backlash and poor journalistic ethics. Some Indian channels such as Zee News falsely claimed that the Indian army had captured Islamabad, while India Today and Deccan Chronicle reported that a Pakistani plane had been shot down, fuelling misinformation and public anxiety.

International Reactions and Global Concerns

When the sky turned out to be full of drones and lights: South Asia's first taste of sixth-generation warfare. The international community reacted to the India-Pakistan cyber conflict with concern, urging de-escalation and protection of civilian infrastructure. The UN, US, China, and Russia

called for restraint, while cybersecurity experts treated it as a case study in hybrid warfare. Global tech companies and cybersecurity firms tracked the situation, providing threat advisories and mitigation services. The conflict highlighted the need to strengthen global cyber defense standards and respect international norms. The episode highlighted the importance of cyber warfare in global security and diplomacy, emphasizing the need for a more robust international framework. While experts agree that future conflicts will involve parallel cyberattacks and information battles. As South Asia entered the era of Ghost Warfare.

Notably, Pakistani shot down six Indian aircraft, including three Rafales, SU-30s and Mig-29s, PLUS (6+1), an Israeli-made Heron UAV by J-10Cs and JF-17s., this is a significant achievement for Chinese aviation technology as significant surge in the price of Chengdu Aircraft Corporation's stock. in addition to demonstrating the Pakistan's air superiority and operational competence, this conflict showcased the strategical decision-making capacity. Pakistan has provided proof by playing intercepted Rafale radio communications, and showed its electronic superiority live, during a military press conference. Pakistan did all this in self-defence and to secure regional peace, and gained global support. On the other side except Israel, no other state supports this cruel act of India. However this war also deflated the "incredible India "bubble that driven by Modi's people (Hussain, 2025).

Pakistan was forced to respond with air strikes to deter further Indian aggression. A deterrence approach requires proven combat capabilities and resolve. Pakistan is capable of fighting both conventional and nuclear wars. In all likelihood, he failed to stop India's offensive on May 7. A counterattack should be launched to demonstrate his determination to fight to restore deterrence stability between Pakistan and India (Jaspal, 2025).

Sixth generation warfare emphasizes non-contact warfare, cyber tools, economic sabotage, and psychological operations, redefining modern conflicts. Furthermore, these are key factors that make winning difficult. With a combination of static and limited kinetic (physical) activities, the 2025 war was a prime example of 6GW. However, the two states are engaged in an economic war and have suspended trade agreements. Furthermore, the

conflict has spilled over into cricket, a symbol of the deep-seated animosity. Unlike past wars, this conflict has had no clear end, with ongoing skirmishes and narrative battles.

Conclusion and Policy Recommendations

However, this four-day war between Pakistan and India highlighted the complexities of deterrence in South Asia. India used coercive diplomacy towards Pakistan and in respond, Pakistan used conventional deterrence policy. But the six generational warfare confirms that there's no space for conventional war between nuclear powers. Pakistan's "Marka-e-Haq" campaign framed strikes as justice and sovereignty while India's "Sindoor" symbolized the narrative of punishing innocent blood. Moreover, deterrence was secured, not by stealth, but by robust mechanisms. However, the India-Pakistan conflict demonstrated the power struggle of realism and the narrative war of constructivism. In short, digitalization in this nuclear age demands a rejection of the ideologies that normalize military adventures and cyber ventures. Therefore, cyber deterrence is also crucial as autonomous technologies redefine the traditional battlefield, which could lead to nuclear war. The conflict confirms that deterrence is about measured capability, not performative risk, as military, economic and digital become all-in-one 6GW or knowledge weapons to influence the enemy. However, both states should organize exchange programs as cultural diplomacy. Furthermore, power without conscience is a warning and we cannot ignore it. The international community should legislate to avoid the implications of a six-generation war to control artificial intelligence in the military, economy and cyber domain. A human perspective should be used in decision-making rather than AI because it is a matter of national security of the state and human dignity. As machines lack the human capacity for empathy and intrinsic respect for human life. Last but not least, to avoid psychological manipulation, states should introduce rules that people with professional certificates can speak in major areas such as security, finance, law and education. This policy can reduce misinformation, disinformation, and cyber fraud/attacks. The controversy exposed gaps in coordination and the need for a robust cyber defense framework. There

should global cyber warfare agency who sign agreement and make clear rules for cyber defense and offense. Misunderstandings and misinformation can be spread through cyber operations, especially when it comes to attribution. As a result, timely communication is crucial during a cyber crisis. The two countries can exchange ideas, ensure technical cooperation, and maintain a directory in case of a crisis. However, Cyber CBMs, such as hotlines and dedicated points of exchange, have the potential to improve predictability.

REFERENCES

- Affairs, P. M. (2025, May 7). Pakistan Strongly Condemns India's Blatant Aggression. Retrieved from mofa.gov.pk: <https://mofa.gov.pk/press-releases/pakistan-strongly-condemns-indias-blatant-aggression>
- Ali, N. (2025, May 12). Pakistan's Sixth-Generation Warfare. Retrieved October 2, 2025, from The Nation: <https://www.nation.com.pk/12-May-2025/pakistan-s-sixth-generation-warfare>
- Allyn, B. (2022, March 16). Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn. Retrieved from NPR: <https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia>
- Andreopoulos, M. (2025, June 03). Turkey and Drone Warfare in the Pakistan-India Conflict. Retrieved October 17, 2025, from The Geopolitics: <https://thegeopolitics.com/turkey-and-drone-warfare-in-the-pakistan-india-conflict/>
- APP. (2025, August 12). Role of Information Ministry in countering enemy's propaganda will always be remembered: Tarar. Retrieved September 24, 2025, from Associated Press of Pakistan: <https://www.app.com.pk/national/role-of-information-ministry-in-countering-enemys-propaganda-will-always-be-remembered-tarar/>
- Ashraf, N. (2025). The Paradox of Cyber Warfare and Clausewitz's Conception of War. NUST Journal of International Peace & Stability, 8(1), 17-29.

- Baek, D. S. (2025, May 14). Cyber Warfare in the May 2025 India-Pakistan Conflict. Retrieved from LinkedIn: <https://www.linkedin.com/pulse/cyber-warfare-may-2025-india-pakistan-conflict-david-sehyeon-baek-ygjoc>
- Biswas, S. (2025, May 09). The first drone war opens a new chapter in India-Pakistan conflict. Retrieved October 12, 2025, from BBC: <https://www.bbc.com/news/articles/cwy6w6507wqo>
- Burkey, M. T. (2025). How Quantum Sensing Will Help Solve GPS Denial in Warfare. California: Lawrence Livermore National Laboratory .
- Desk, b. t. (2025, october 29). Pak airspace closure had an impact of ₹4,000 crore': Air India CEO Campbell Wilson says Europe, US routes were hit. Retrieved 02 November, 2025, from business today: <https://www.businesstoday.in/india/story/pak-airspace-closure-had-an-impact-of-rs4000-crore-air-india-ceo-campbell-wilson-says-europe-us-routes-were-hit-500006-2025-10-29>
- Ding, C. (2016, September 10). China Launches World's First Quantum Telecommunication Satellite. Retrieved from Yale Scientific: <https://www.yalescientific.org/2016/09/china-launches-worlds-first-quantum-telecommunication-satellite/>
- Fildes, J. (2010, september 23). Stuxnet worm 'targeted high-value Iranian assets'. Retrieved from BBC: <https://www.bbc.com/news/technology-11388018>
- Haddad, M. (2023, May 23). Fake Pentagon explosion photo goes viral: How to spot an AI image. Retrieved from Al Jazeera: <https://www.aljazeera.com/news/2023/5/23/fake-pentagon-explosion-photo-goes-viral-how-to-spot-an-ai-image>
- Hussain, A. (2025, May 13). 25 Things We Learned from the Pakistan-India War of 2025. Retrieved from LinkedIn: https://medium.com/@amirhusain_tx/25-things-we-learned-from-the-pakistan-india-war-of-2025-ba7f9345d5e0
- Israel Aerospace Industries HAROP loitering munition. (2023, November 23). Retrieved from automatedresearch.org: <https://automatedresearch.org/weapon/israel-aerospace-industries-harop-loitering-munition/>
- Jaspal, D. Z. (2025, May 13). Ironically, Pakistan's heavy retaliation to Indian strikes was important to uphold deterrence stability. Retrieved Novemebr 3, 2025, from Arab News: <https://www.arabnews.pk/node/2600597>
- Lakshmanan, R. (2021, May 9). Ransomware Cyber Attack Forced the Largest U.S. Fuel Pipeline to Shut Down. Retrieved from The Hacker News: <https://thehackernews.com/2021/05/ransomware-cyber-attack-forced-largest.html>
- Mansoor, A. (2025, May 10). Hackers leak sensitive Indian defence data on dark web. Retrieved October 22, 2025, from 24 News: <https://24newshd.tv/10-May-2025/hackers-leak-sensitive-indian-defence-data-on-dark-web>
- Mogul, R., Iyer, A. S., & Saifi, S. (2025, April 24). A tourist massacre in Kashmir is escalating tensions between India and Pakistan. Here's what we know. Retrieved October 2, 2025, from CNN: <https://edition.cnn.com/2025/04/24/india/pahalgam-india-pakistan-attack-explainer-intl-hnk>
- Reports, I. (2025, May 11). India-Pakistan Conflict 2025: Fighter Jets, Missiles, and Drones. Retrieved from IRIA Reports: <https://www.ir-ia.com/India-Pakistan-Conflict-2025.html>
- Shah, S., & Patel, S. (2025, August 2). How Pakistan shot down India's cutting-edge fighter using Chinese gear. Retrieved October 06, 2025, from Reuters: <https://www.reuters.com/business/aerospace-defense/how-pakistan-shot-down-indias-cutting-edge-fighter-using-chinese-gear-2025-08-02/>

- Shahzad, A., Shahid, A., & Bukhari, F. (2025, April 24). Pakistan closes air space for Indian airlines, warns against water treaty violation as ties plummet. Retrieved September 20, 2025, from Reuters: <https://www.reuters.com/world/india/india-calls-all-party-meet-summons-top-pakistani-diplomat-after-kashmir-attack-2025-04-24/>
- team, A. (2025, May 12). Pakistan's response to be decisive if sovereignty threatened: DG ISPR. Retrieved September 8, 2025, from Aaj: <https://english.aaj.tv/news/330416023/pakistans-response-to-be-decisive-if-sovereignty-threatened-dg-ispr>
- Team, R. P. (2025, May 10). Majority of Indian websites hacked in Pakistani cyber attack. Retrieved from Radio Pakistan: https://radio.gov.pk/10-05-2025/majority-of-indian-websites-hacked-in-pakistani-cyber-attack#google_vignette
- Team, T. (2025, May 15). Security sources reveal details of Pakistan's massive cyberattack against India. Retrieved October 4, 2025, from Tribune: <https://tribune.com.pk/story/2546050/security-sources-reveal-details-of-pakistans-massive-cyberattack-against-india>

