International Journal of Research Studies on Environment, Earth, and Allied Sciences (IJRSEAS)
| Volume-2 Issue-4 |August-2025 | ISSN: 3066-0637 | Website: https://eesrd.us

Manuscript ID:
IJRSEAS-2025-020403

OPEN ACCESS

Quick Response Code:

Website: https://eesrd.us

DOI: 10.5281/zenodo.17589933

DOI Link:
https://doi.org/10.5281/zenodo.17589933

Volume: 2

Issue: 4

Pp. 10-13

Month: August

Year: 2025

E-ISSN: 3066-0637

Submitted: 06 July 2025

Revised: 10 July 2025

Accepted: 10 Aug. 2025

Published: 31 Aug. 2025

Address for correspondence:
Dr. Nipan Haloi
Assistant Professor, Department of Political Science, Sankardeva Mahavidyalaya, Pathalipahar, Lakhimpur, Assam
Email: niponhaloi21@gmail.com

How to cite this article:
Haloi, N. (2025). Understanding the Changing Nature of Conflict: A Study of GPS spoofing. International Journal of Research Studies on Environment, Earth, and Allied Sciences, 2(4), 10–13.
https://doi.org/10.5281/zenodo.17589933

Understanding the Changing Nature of Conflict: A Study of GPS spoofing

Dr. Nipan Haloi
Assistant Professor, Department of Political Science,
Sankardeva Mahavidyalaya, Pathalipahar, Lakhimpur, Assam

Abstract

Conflict has been an enduring aspect of human society, shaping civilizations and influencing the course of history. In the contemporary era, however, the nature of conflict has undergone a fundamental transformation, moving away from conventional interstate wars to more complex intrastate struggles, insurgencies, terrorism, cyber warfare, and identity-based violence. This study, descriptive in nature and based entirely on secondary sources, explores the changing character of modern conflict and examines the emerging challenge of Global Positioning System (GPS) spoofing as a tool of electronic warfare. Drawing on the theoretical insights of Mary Kaldor's "new wars," Bruce Hoffman's work on terrorism, and recent scholarship on hybrid warfare, the paper analyses how technology, information manipulation, and the rise of non-state actors have blurred the lines between combatants and civilians, expanding the battlefield into cyberspace and urban centers. The paper further highlights GPS spoofing as a critical manifestation of modern conflict, with profound implications for aviation safety, national security, and regional stability. Recent incidents in the Middle East and South Asia demonstrate the disruptive capacity of spoofing to mislead navigation systems, conceal cross-border movements, and threaten both civilian and military operations. In the Indian context, the growing reliance on satellite navigation raises urgent questions about vulnerabilities in national defense, cyber infrastructure, and aviation frameworks. The study argues that conflict resolution mechanisms must evolve in response to these challenges by integrating traditional approaches such as mediation and dialogue with modern tools like data analytics, artificial intelligence, and digital platforms. At the same time, addressing threats like GPS spoofing requires proactive strategies that combine technological innovation, international cooperation, and strong governance. Ultimately, resilience, inclusivity, and foresight remain the most effective tools for sustaining peace in an era of increasingly complex and technologically driven conflicts.

Keywords: *Conflict Transformation, Hybrid Warfare, GPS Spoofing, National Security*

Introduction

Conflict has been a perennial feature of human history. The term conflict is normally is used for fight, debate, argument, contest, war, clashes between or among groups, terrorism, insurgency, religious extremism and other similar acts. In fact, conflict has been an integral part of human affairs. Since the historical times, when human being started living in groups, human civilisation has evolved through a complex process of conflict and attempts to find ways to manage and resolve it. This study examines the changing nature of modern conflict, specifically analysing the use of methods such as digital spoofing and their broader implications.

Objective

1. To understand the changing nature of modern conflict.
2. To look at GPS spoofing and its wider implications.

Methodology

This study is descriptive in nature and relies exclusively on secondary sources of data. It employs a qualitative approach that seeks to understand and explain the changing nature of modern conflict and the emerging challenge of GPS spoofing within the larger framework of contemporary security studies. The analysis has been carried out through an extensive review of existing literature, including books, journal articles, government reports, official statements, think tank publications, and credible media accounts. Theoretical perspectives such as Mary Kaldor's concept of "new wars," Bruce Hoffman's insights on terrorism, and contemporary studies on hybrid warfare and cyber threats have been integrated to provide a conceptual foundation for the research. Since the study is based only on secondary data, it does not involve fieldwork or the collection of primary evidence. Nevertheless, by synthesizing diverse perspectives and contemporary evidence, the study offers a comprehensive framework for examining the changing character of conflict and the urgent need to address technological threats such as GPS spoofing.

The changing nature of conflict

Modern conflict has undergone a profound transformation, shifting from traditional interstate wars to intrastate conflicts such as civil wars, insurgencies, and localized violence, which now dominate global armed struggles. Mary Kaldor's "new wars" thesis provides valuable insights into the changing dynamics of warfare, emphasizing the increasing impact on civilians and the blurred lines between battlefronts and civilian spaces (Kaldor, 1999).

A defining feature of contemporary conflict is the rise of non-state actors such as armed groups, insurgents, terrorist organizations, and private military contractors. As Bruce Hoffman notes in Inside Terrorism, groups like ISIS, Hezbollah, and the Wagner Group exemplify this trend (Hoffman, 2017). Furthermore, modern warfare increasingly takes the form of hybrid warfare, a concept explored by Linda Robinson et al., which combines conventional, irregular, cyber, and information operations to achieve strategic objectives without triggering full-scale war (Kofman, 2017). Apart from that Kim Zetter describes in Countdown to Zero Day, modern conflict includes attacks on digital infrastructure, data breaches, surveillance, and misinformation campaigns, often blurring the lines between military and civilian targets.

The weaponization of information has further intensified conflict, with states and non-state actors using social media, propaganda, and fake news to manipulate public opinion and destabilize societies. The alleged Russian interference in the 2016 U.S. elections through online disinformation is a prime example of this psychological warfare (U.S. Senate Select Committee on Intelligence, 2019). Additionally, modern conflicts are increasingly urban, with battles fought in densely populated cities like Aleppo, Gaza, and Mosul, resulting in high civilian casualties and massive infrastructure damage. The International Committee of the Red Cross reports that urban warfare leads to eight times more civilian deaths than rural conflicts (International Committee of the Red Cross, 2015). Another notable shift lies in the motivations driving conflict: while traditional wars were often about territory or power, contemporary conflicts are frequently fueled by identity, ethnic, religious, or ideological making them harder to resolve. Lastly, the role of technology has become central, as highlighted by Peter Bergen and Daniel Rothenberg in Drone Wars (Bergen and Rothenberg, 2015).

GPS spoofing and its broader implications

GPS spoofing has emerged as one of the dangerous activities carried out by certain countries in recent times, with serious adverse implications. GPS spoofing is a deceptive cyber technique that manipulates Global Positioning System (GPS) data by transmitting false signals to mislead a GPS receiver about its real location. This poses significant risks to aviation, especially for civilian aircraft that depend heavily on GPS for navigation and landing. Spoofing prevents flight systems from receiving accurate, real-time data, endangering flight safety (Shahid, 2025). The recent geopolitical tensions in the Middle East especially Israel's efforts to defend against missile attacks have brought renewed attention to the risks associated with GPS spoofing ("Israel's Attacks and GPS Spoofing", 2025). While Israel's use of electronic warfare aims to confuse and deflect hostile missile systems, such tactics may have unintended side effects on global navigation systems. As GPS spoofing becomes more common, countries like India, which increasingly rely on GPS for both civilian and military operations, could be vulnerable to significant disruptions.

A September 2024 report by the OPS Group highlighted widespread spoofing activity linked to Israel, affecting even areas as distant as northwest New Delhi and Lahore ("Are Israel's GPS Attacks Impacting India", 2025). During the one-month period from July 15 to August 15, 2024, 316 aircraft were impacted in this region alone. In March 2025, the Indian government officially acknowledged in the Lok Sabha a disturbing rise in GPS interference and spoofing incidents reported along the Amritsar and Jammu air corridors (Awasthi, 2025). The report revealed a 500% surge in spoofing cases in 2024, with over 70% of surveyed flight crews expressing serious safety concerns. Hotspots such as the Eastern Mediterranean, Black Sea, and parts of Asia have seen over 1,000 flights affected in August 2024 alone.

Overall, these spoofing resulted in tactical disruption, operational concealment, and strategic messaging causing immediate confusion in controlled airspace and hiding unauthorized cross-border movements. Ultimately, such actions can impact a nation's strategic posture and security capabilities. Therefore, several critical questions arise in light of the growing threat of GPS spoofing. What is the impact of such spoofing activities on civil aviation safety in India and its surrounding regions? Given India's increasing reliance on satellite navigation, how might these disruptions affect national security and military preparedness? Furthermore, there is a pressing need to examine the technological gaps within India's existing GPS-based infrastructure and assess the country's capacity to detect, respond to, and mitigate spoofing attacks. Equally important is evaluating the robustness of India's aviation and cybersecurity frameworks in addressing these evolving challenges. Finally, the situation demands an exploration of the legal and diplomatic instruments available to India to identify and hold accountable those actors responsible for deploying GPS spoofing as a tool of electronic warfare.

Mechanisms of Conflict Resolution

The mechanisms of conflict resolution have evolved significantly in response to the changing nature of conflict in the modern world. Unlike traditional disputes between states, today's conflicts are often complex, multi-dimensional, and deeply rooted in issues such as inequality, marginalization, governance deficits, and resource scarcity. As a result, traditional methods like diplomacy or military intervention alone are no longer sufficient to bring about long-term stability. Modern conflict resolution requires a combination of innovative approaches that not only aim to stop violence but also address its underlying causes. Addressing root causes is one of the most critical aspects of sustainable conflict resolution. Conflicts are often born from long-standing structural inequalities,

political exclusion, or the absence of good governance. Therefore, policies and interventions must tackle these deep-seated issues by promoting social justice, political participation, and equitable economic opportunities. Empowering civil society also plays a vital role in this process, as community-led peace initiatives tend to be more inclusive and sustainable. Civil society organizations can bridge the gap between communities and governments, fostering trust, dialogue, and grassroots participation in peacebuilding. Alongside this, mediation and arbitration have become indispensable tools in international and domestic conflicts. Neutral third parties, such as the United Nations, the World Trade Organization, or regional organizations, often mediate disputes and provide platforms for fair negotiation. These mechanisms create space for parties to come to the table and find solutions without resorting to violence. Dialogue and negotiation remain at the heart of conflict resolution, as engaging all stakeholders—including governments, corporations, and civil society—in constructive discussions is essential to building consensus and achieving mutually acceptable solutions.

In addition, post-conflict peacebuilding and reconciliation are critical for ensuring that peace endures. Stopping the violence is only the first step; rebuilding societies requires addressing the trauma of war, fostering reconciliation between divided groups, ensuring justice for victims, and promoting socio-economic development so that communities can rebuild their lives. Peacebuilding efforts that incorporate education, healthcare, and employment opportunities are particularly effective in preventing the recurrence of violence. Furthermore, in the twenty-first century, technology and innovation have become powerful tools in the field of conflict resolution. Advancements in data analytics, artificial intelligence, and digital communication allow governments, NGOs, and international organizations to predict potential conflicts, monitor real-time developments, and facilitate dialogue across geographical and cultural divides. For example, data-driven conflict mapping can highlight flashpoints before they escalate, while digital platforms enable communities to share grievances and resolve misunderstandings more effectively. Technology also enhances transparency and accountability, reducing the likelihood of miscommunication or manipulation. Taken together, these advanced mechanisms underscore the importance of moving beyond reactive approaches to conflict and adopting proactive, inclusive, and innovative strategies. Only by addressing both the visible manifestations and the invisible root causes of conflict can societies hope to build lasting peace in an increasingly interconnected and turbulent world.

Conclusion

The changing nature of conflict is both a challenge and a call to innovation in global governance, security policy, and peacebuilding. Warfare is no longer confined to battlefields; it permeates cyberspace, city streets, and social media platforms. The rise of non-state actors, the influence of digital technologies, and the primacy of identity over ideology have fundamentally altered the conduct and consequences of war. To address these evolving dynamics, the global community must embrace flexible, multidisciplinary strategies that combine military readiness with conflict prevention, human rights advocacy, and technological regulation. The imperative is clear: in an era of complex threats, resilience, cooperation, and foresight are our best tools for sustaining peace.

Apart from that addressing the threat like GPS spoofing, India must adopt a proactive, multidimensional strategy that integrates technological innovation and strategic policies. GPS spoofing is a quiet but serious threat to India's flight safety, border protection, and national control. The Government of India must invest in producing an indigenous low-cost general-purpose NavIC receiver for resilient GNSS technologies and anti-spoofing technologies that are not dependent on foreign hardware, particularly Chinese hardware. Although the challenge is complex, it can be handled. By using better technology, staying alert during operations, working with other countries, and building strong defenses, India can protect itself from this growing electronic threat.

Acknowledgement

I am highly grateful to the Principal of Sankardeva Mahavidyalaya for the encouragement extended to me in carrying out my research work.

Financial Support and Sponsorship

Nil.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Kaldor, Mary. (1999). *New and old wars: organized violence in a global era*, Stanford, Calif.: Stanford University Press.
2. Hoffman, Bruce. *Inside Terrorism*, 3rd ed. (2017) New York: Columbia University Press, 2, Pp. 45–67.
3. Kofman, Michael et al., (2017) *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, CA: RAND Corporation.
4. U.S. Senate Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election (Washington, DC, 2019).
5. International Committee of the Red Cross, "Urban Services During Protracted Armed Conflict: A Call for a Better Approach to Assisting Affected People," ICRC, 2015.
6. Bergen, Peter and Rothenberg, Daniel eds., (2015). *Drone Wars: Transforming Conflict*, Law, and Policy, New York: Cambridge University Press.
7. Shahid, Gazi Abbas. (2025). "Israeli attacks dangerous for India?", *India.com*, Retrieved from https://www.india.com/news/world/gps-spoofing-israeli-attacks-dangerous-for-india-report-says-this-israeli-

technology-threatening-security-of-indias-aircraft-can-impact-pakistan-border-due-to-plane-crash-india-israel-relations-7706499/
8. "Israel's Attacks and GPS Spoofing: How It Could Impact India", *Bharat Articles*, March 25, 2025, Accessed from https://bharatarticles.com/israels-attacks-and-gps-spoofing-how-it-could-impact-india/
9. "Are Israel's GPS Attacks Impacting India as It Records 465 Incidents Of "GPS Spoofing" In Last 15 Months?" *EURASIAN TIMES*, March 24, 2025. Retrieved from https://www.eurasiantimes.com/rising-threat-of-gps-spoofing-in-global-aviation/
10. Awasthi, Soumya. (2025). "Securing India's Skies: Countering the Threat of GPS Spoofing and Hybrid Warfare", *Observer Research Foundation*, Expert Speak Raisina Debates.