iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** I **Month of publication:** January 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.77212

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue I Jan 2026- Available at www.ijraset.com*

# Grey-Zone Warfare in the Age of Artificial Intelligence

Shriniwas Gunwant Raje[1]
[1]*MA in International Relations and Security Studies, SICSSL, Rashtriya Raksha University, Gandhinagar, Gujarat, India*

***Abstract:*** ***The contemporary international security environment is increasingly shaped by competition that unfolds below the threshold of open armed conflict. Commonly described as grey-zone warfare, this mode of contestation relies on ambiguity, deniability, and gradual escalation to achieve strategic objectives while avoiding direct military confrontation. At the same time, artificial intelligence has emerged as a transformative technology that reshapes how power is exercised across political, informational, cyber, and physical domains. This paper argues that artificial intelligence functions as a structural enabler of grey-zone warfare by lowering operational costs, enhancing precision and persistence, and obscuring attribution and intent. Rather than merely augmenting existing tactics, AI fundamentally alters the logic of sub-threshold conflict, making continuous competition both feasible and strategically attractive. Through conceptual analysis and an examination of real-world incidents, particularly AI-enabled information and cyber operations in the Russia–Ukraine context prior to 2022, this study demonstrates how AI intensifies grey-zone dynamics while undermining traditional deterrence, legal accountability, and strategic stability. The paper concludes by assessing the broader implications of AI-driven grey-zone warfare for global security governance and the future of conflict.***

***Keywords: Grey-Zone Warfare, Artificial Intelligence in Security, Hybrid Conflict, Cyber and Information Operations, Strategic Competition, Attribution and Deterrence.***

## I. INTRODUCTION

The nature of conflict in the twenty first century is becoming more influenced by the sustained strategic rivalry that takes place below the conventional armed conflict level. In contrast to the conflicts of the twentieth century, involving decisive battles, the conquest of the territory, and the declaration of the war, the rivalry of geopolitical opponents in the modern world exists in an ongoing environment between the peace and open warfare. Nuclear deterrence, economic globalization, interdependence through diplomatic ties and the development of international law practices have placed a limiting role on the emergence of large-scale interstate wars [1]. Nonetheless, lack of open warfare has not meant that there is no rivalry between the leading powers, but rather competition has been turned to less open and more oblique and non-acknowledgement forms of interactions. States and non-state actors now actively engage in strategically intending actions that are aimed at ensuring that they do not provoke a conventional military reaction and at the same time bring a significant pressure bearing political, economic, informational, or security implications. These actions tend to be conducted in legally grey spaces, take advantage of institutional and normative loopholes and use gradual escalation to gain incremental benefit without attracting the full-scale backlash [2]. This is a changing form of conflict commonly referred to as grey-zone warfare and is a continuum of strategies that falls short of armed conflict but are beyond normal diplomatic or economic competition. Grey-zones focus on ambiguity, deniability, perseverance, and psychological pressure instead of military force. Working between the war and peace, grey-zone actors are pursuing the goal of redefining the perceptions of adversaries, undermining their institutional stability, and changing the balance of strategies without crossing red lines that would offer direct military action. Consequently, grey-zone war has become the characteristic trait of international relations today, which radically redefines the manner, in which the international security environment competes and exercises power in the modern globalized world as illustrated by N. kumar [3].

Practically, the grey-zone warfare has turned into a prevalent tool of statecraft in the modern security competition, thus becoming more and more blurry on the boundaries between military and civilian space, control over the domestic and foreign spheres of influence, as well as peace and conflict. Instead of the fast territorial expansion or a critical victory on the battlefield, grey-zone campaigns aim to undermine the political unity, institutional validity, economic viability, and popular confidence of the adversary over a long period of time [4]. These tactics entail various instruments such as computer intrusions, disinformation operations, financial coercion, proxy forces, legal warfare, and targeted military signalling into integrated and long-range operations aimed at ensuring accrual of incremental benefits and plausible deniability.

There are significant cases of the increased popularity of grey-zone strategies in international relations. The preceding operations by Russia against Ukraine before 2022 consisted of synchronized cyberattacks, information warfare, politically influenced campaigns, and proxy fighting in Crimea and Donbas, which only indicates a long-term ambition to influence the formation of strategic consequences without any instant conventional increase [5]. Based on this changing strategic environment, this paper reviews the aspect of artificial intelligence (AI) as a new enabler of grey-zone warfare. The paper takes a conceptual and empirical way of assessing the role of AI-enabled abilities in enhancing ambiguity, persistence, and deniability in modern war.

The scope of this paper is structured around four key analytical dimensions:

*1)* The strategic integration of AI into grey-zone operations and sub-threshold conflict models;
*2)* Empirical analysis of AI-enabled information and cyber campaigns in recent geopolitical cases;
*3)* Implications for deterrence, attribution, legal accountability, and strategic stability;
*4)* Governance, ethical, and policy challenges arising from the normalization of AI-mediated competition.

## II. THE STRATEGIC LOGIC OF GREY-ZONE WARFARE

Ambiguity and incremental escalation as well as continued pressure characterize grey-zone warfare, which is a strategic rationale that prefers ambiguity over an actual military conflict. They avoid crossing over very clear red lines and opt instead to exploit political, legal, informational, cyber, and economic vulnerabilities to inflict incremental costs against their adversaries with no plausible deniability (grey-zone actors) [6]. This approach allows the states (and non-state actors) to follow strategic objectives in the ambiguous situation when attribution is disputed and the reaction is restricted by the rule of law and norms. The grey-zone operations provide confusion in determining whether it is a state of peace or state of conflict, and place the ancient paradigms of deterrence and crisis management in an awkward situation, combining civilian and military operations, open, secret operations, and official and proxy operations. This kind of war is destabilizing institutional practices, social cohesiveness, and the strategic environment without the provocation of open war, gray-zone warfare is becoming a constant and structural feature of the contemporary international security [7].

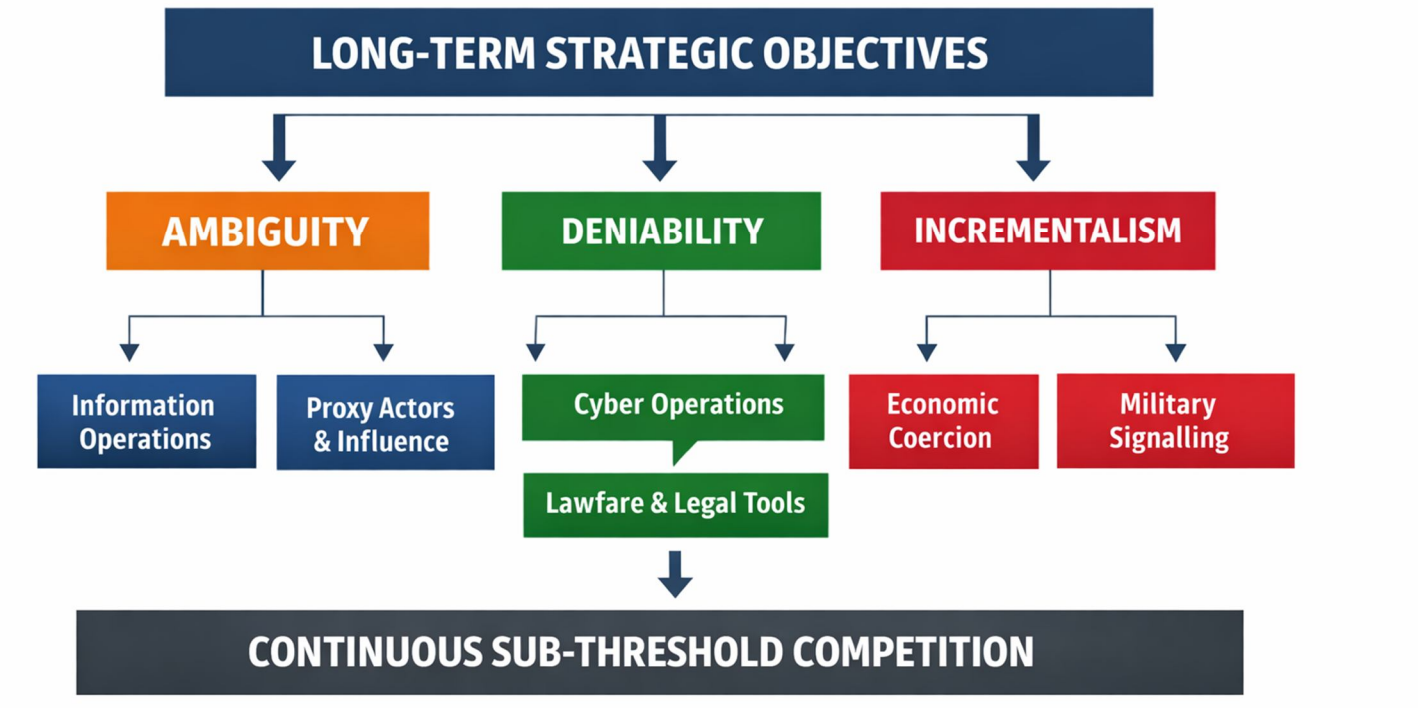



Figure 01: Strategic Architecture of Grey-Zone Warfare (Conceptual Framework)

To further this line of thought, grey-zone warfare is rooted in multi-domain campaigns and not in the unitary tactic operations. The actors manipulate information to shape the way the people are seen, spy or disrupt through cyber operations, leverage the economy to influence political decision making and use proxy networks so that they cannot be directly held accountable [8].

Digital technology and the development of artificial intelligence are other factors that help to make the effectiveness of grey-zone even greater by providing the opportunity to scale the influence operations, micro-target behavior, auto-deception, and expedited decision-making [9]. It is important to note that these strategic approaches leverage the constraints of the institutions, norms of democracy and legislation of target states that create asymmetric advantages of slow, cumulative strategic benefits in comparison with instant opposition. The traditional structures of deterrence, international legal practices, and stability in the international politics face a greater challenge as the element of the competitive aspect is injected into the everyday political, economic and informational interaction [10][11].

TABLE 1
STRATEGIC MECHANISMS OF GREY-ZONE WARFARE WITH REAL-WORLD EXAMPLES

| Strategic Mechanism | Description | Primary Objective | Notable Example |
|---|---|---|---|
| Plausible Deniability | Concealing or obscuring actor responsibility | Avoid retaliation and escalation | Russia's covert operations in Crimea (2014) |
| Incremental Escalation | Gradual pressure to avoid military thresholds | Secure slow strategic gains | China's expansion in the South China Sea |
| Information Warfare | Disinformation, propaganda, and narrative shaping | Influence public opinion and political stability | Election interference campaigns in Western democracies |
| Cyber Operations | Digital espionage, disruption, and infrastructure intrusion | Intelligence extraction and coercion | SolarWinds cyber intrusion (2020) |
| Economic Coercion | Trade pressure, sanctions, and financial leverage | Influence national policy decisions | China–Australia trade restrictions |
| Proxy Warfare | Use of allied militias or non-state actors | Reduce attribution and direct risk | Iran-backed proxy groups in the Middle East |
| Lawfare | Manipulating legal systems and international norms | Legitimize territorial or political claims | China's maritime legal assertions |
| Military Signalling | Limited shows of force and calibrated exercises | Deter, intimidate, or coerce | North Korean missile testing |
| Social Engineering | Psychological manipulation exploiting human trust | Gain access, extract intelligence, or influence behavior | Phishing campaigns targeting government agencies |
| LLM-Enabled Attacks | Use of large language models to automate persuasion, phishing, or misinformation | Scale deception and influence operations | AI-generated spear-phishing and deepfake political messaging |

## III. ARTIFICIAL INTELLIGENCE AS A STRUCTURAL ENABLER OF GREY-ZONE CONFLICT

Artificial intelligence is transforming the grey-zone conflict not just in regard to the instrumentation of the projection of it, but also in regard to the form of the power possessed by it. Rather than simply accelerating the strategies already in place, AI changes the individuals who may be acted on, the tempo of activity, the affordability with which control may be impose and the challenging nature of discerning or attributing malicious action.

It transforms the structural character of grey-zone competition: the activities are more continuous, more scalable, less apparent and hard to dishearten. With the help of AI, actors can conduct long-term low-intensity campaigns on the information, cyber, economic, and political front without the presence of huge military forces and with no obvious escalation of the situation. This leads to the grey-zone war turning into a kind of data-driven, automated and algorithmically optimized competition, where influence and disruption becomes possible cheaply and with little risk of political blowback at a low cost and risk of political blowback to the politics [12].

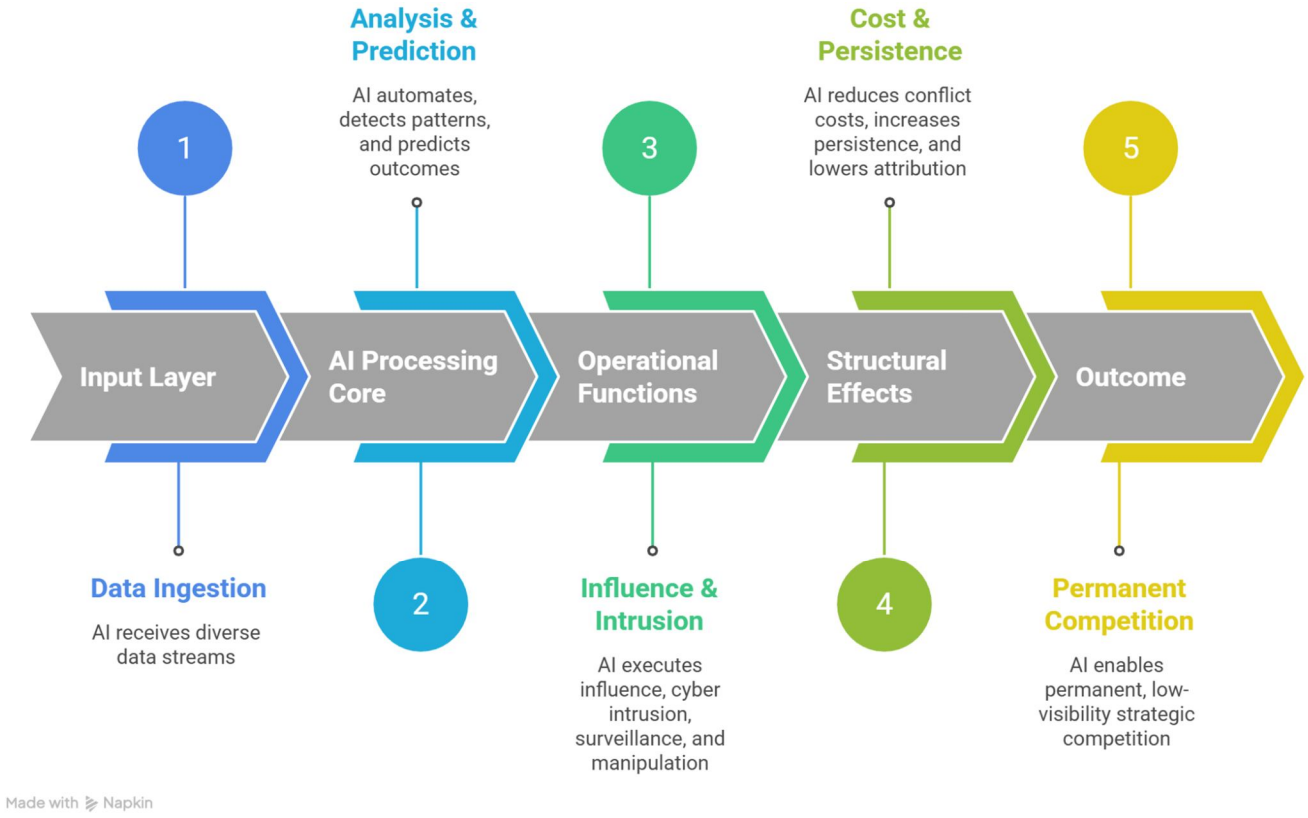



Figure 2: Structural Role of AI in Transforming Grey-Zone Conflict

The grey-zone conflict supported by AI is the structural form of the previous forms of hybrid warfare, which places the operational functions previously dependent on human cognition, discretion and intent in automated and algorithm maximizing operations. This modification alters the strategic aspects of sub-threshold competition so that the operations become quicker, scalable, persistent, and deniable besides rendering the operations less costly and the human risk less vital. Operations like producing mass propaganda, real-time narrative generation, psychological profiling of a group of people, finding cyber vulnerabilities, and optimization of influence via continual feedback learning is now automated. High-volume and personalized persuasion and social engineering are executed by means of Large Language Models, predictive targeting, campaign calibration, and forecasting adversary behavior are performed by using machine-learning systems [12,13]. Organizational attributes of these capabilities basically reduce decision-making processes, saturation of defensive abilities, attribution processes, which reduces the efficacies of conventional deterrence arrangements and responsibility frameworks. What this functionally produces is the transformation of the dynamic of episodic encounter based on crisis to long-term, low-profile pressure on strategy that is exerted less than predetermined levels of escalation.

Regarding the theoretical perspective of International Relations, AI-enabled grey-zone action entrenches the dynamics of realism, which involve the capacity of states to pursue power, influence without necessarily taking the risk of an overt military confrontation. At the same time, the liberal institutionalist mechanisms have constraints to manage the operations meditated by AI since they are not active on gaps in enforcement, normative lags, and jurisdiction fragmentation.

Constructivist dynamics complicate response efforts, as well because manipulation of the narrative by AI characters changes the political identity, the perception of the threat, and the legitimacy discourses. These processes on the systemic level apply to the establishment of a climate in which sub-threshold competition becomes customized, programmed, standardized into the mechanism of world political interaction. It is a structural, institutional and cognitive framework of constraints which in many cases can deny states the opportunity to detect, attributing, or reacting to the AI-enabled grey-zone operations. The proliferation of AI-powered processes on civilian system complicates the process of prosecuting the offender of this type of actions and delegitimize the legal and diplomatic framework within which revenge could be unleashed. Bureaucratic divisiveness and the slowness of the interagency coordination process inhibits the necessity to respond swiftly to high velocity automated campaigns, and the domestic legal and normative safeguard, at least democratic ones, curtails mass-scale monitoring and counter-influence activities. Moreover, the outdated deterrence dogmas do not resonate with the homogeneous, non-kinetic, and non-deniable coercion, which reduces the credibility of retaliation and is a sign of success. The policymaking institutions underestimate systemic low-intensity interference further because of cognitive bias. The increasing range of AI-enabled influence, cyber automation, behavioral targeting and decision-optimization capabilities in Table 2 (AI Enablement Pathways - Capabilities, Scope, and Strategic Outcomes) make such vulnerabilities worse by enabling scalable, adaptive, and persistent sub-threshold operations that subvert current deterrence, governance and escalation-control approaches [14].

TABLE 2
AI ENABLEMENT PATHWAYS — CAPABILITIES, SCOPE, AND STRATEGIC OUTCOMES

| AI Enablement Pathway | How AI Is Applied | Operational Scope | Strategic Outcome |
|---|---|---|---|
| Narrative Automation (LLMs) | Generates adaptive propaganda, targeted persuasion, and automated social engineering | Information warfare, psychological influence, election interference | Narrative dominance, polarization, erosion of public trust |
| Synthetic Media & Deepfakes | Produces realistic fake audio/video to mislead or discredit targets | Political coercion, reputation warfare, diplomatic disruption | Delegitimization of leaders, confusion, crisis amplification |
| Autonomous Cyber Operations | Automates vulnerability discovery, intrusion, and lateral movement | Cyber espionage, infrastructure sabotage, IP theft | Persistent access, long-term digital coercion |
| Behavioral Targeting & Profiling | Identifies social fault lines and vulnerable demographic groups | Population influence, protest manipulation, social destabilization | Social fragmentation, amplified unrest |
| Predictive Intelligence & Forecasting | Anticipates adversary reactions and policy shifts | Strategic planning, escalation management, adversary modeling | Preemptive advantage, faster strategic adaptation |
| Automated Economic Manipulation | Analyzes markets and exploits financial vulnerabilities | Sanctions warfare, market destabilization, trade coercion | Economic pressure leverage, policy influence |
| Mass Surveillance & Recognition AI | Tracks individuals, monitors dissent, and controls information flows | Internal repression, counterintelligence, population control | Expanded state coercive capacity, deterrence of opposition |

| | | | |
|---|---|---|---|
| AI-Driven Social Engineering | Crafts hyper-personalized phishing, scams, and insider recruitment | Espionage, credential theft, insider compromise | System access, intelligence penetration |
| Swarm Intelligence & Autonomous Systems | Coordinates semi-autonomous drones or maritime units | Border pressure, maritime grey-zone activity, intimidation | Persistent territorial pressure, coercive signaling |
| Decision-Support & Strategy Optimization | Accelerates operational planning and timing decisions | Military signalling, crisis manipulation, escalation calibration | Faster escalation cycles, reduced human oversight |

## IV. AI ACROSS THE DOMAINS OF GREY-ZONE COMPETITION

Artificial intelligence is increasingly an enabler which is cross-domain and which alters the exercise of power, influence and legitimacy in grey-zone competition in the political, information, cyber, economic and security domains. Altering the traditional state actors, shifting power, decreasing the obstacles to intervention strategies, and turning competition into a fact under the central point of armed conflict, AI is considered through the prism of the International Relations (IR) as changing the existing state functions. Within a realist approach, AI increases the capacity of the states to assume the power by expediting their activities, broadening their sustainability, and minimizing costs in sub-threshold campaigns. The liberal institutionalist perspectives highlight the growing strain that AI puts on the international norms, international governance institutions and international regulatory regimes which are barely in a position to deal with the trans-boundary digital competition. There are also construalist approaches that focus on the reduction of identity, perception and legitimacy by AI due to the ability to manipulate narratives, social meaning and shared trust. With these theoretical insights, AI establishes a foundation of contact between projection of power into construction of legitimacy, normative contestation, restraint of escalation where actors can work on strategic objectives and mitigate the risk of politics and military risks. To make more inroads, exploit institutional weaknesses, and generate a recurring sub-threshold competition, AI permeates across numerous fields as listed in Table 3 ( AI Across Grey-Zone Competition Domains -Roles, IR Values, and Strategic Effects ) [15, 16].

TABLE 3
AI ACROSS GREY-ZONE COMPETITION DOMAINS — ROLES, IR VALUES, AND STRATEGIC EFFECTS

| Domain | AI Applications | IR Role & Value | Strategic Function in Grey-Zone Competition | Key Outcomes |
|---|---|---|---|---|
| Political Domain | AI-driven voter targeting, narrative shaping, policy influence analytics | Legitimacy, regime stability, soft power | Influence domestic politics and foreign policy decision-making | Political polarization, electoral manipulation, legitimacy erosion |
| Information Domain | LLM-based propaganda, deepfakes, narrative automation | Norms, identity construction, perception power | Shape public opinion, control narratives, and influence social cohesion | Trust degradation, narrative dominance, cognitive destabilization |
| Cyber Domain | Automated intrusion, vulnerability scanning, AI malware | Strategic advantage, deterrence signaling, security power | Enable persistent cyber espionage and infrastructure pressure | Intelligence extraction, digital coercion, systemic disruption |
| Economic Domain | Market prediction AI, financial manipulation tools, sanctions optimization | Economic interdependence, coercive leverage | Exploit economic vulnerabilities and influence policy through financial pressure | Trade coercion, market instability, policy concessions |

| | | | | |
|---|---|---|---|---|
| Military & Security Domain | AI-enabled ISR, autonomous systems, decision-support tools | Hard power, deterrence credibility, escalation control | Enhance sub-threshold military signaling and persistent pressure | Coercive deterrence, intimidation, escalation ambiguity |
| Societal Domain | Behavioral analytics, surveillance AI, social engineering automation | Social cohesion, legitimacy, identity stability | Manipulate societal divisions and population behavior | Social fragmentation, unrest amplification, psychological influence |
| Diplomatic & Legal Domain | AI-assisted lawfare, treaty analysis, narrative framing | Norm-setting, legal authority, institutional power | Shape international legal interpretations and diplomatic narratives | Norm exploitation, regulatory asymmetry, institutional strain |

## V. CASE STUDY

In this part, the theoretical backbone to the grey-zone conflict enabled by artificial intelligence would be utilized in the context of life to look into how artificial intelligence is transforming sub-threshold competition in actual strategic situations. Regarding the section, the authors evaluate the use of AI-controlled tools to influence political dynamics, engage in cyber activities, manipulate information spheres, and sustain the force of coercion over an extended period without the use of traditional military pressure escalation. The chosen cases interpret the variation in the capacity of actors, the will to carry out a strategy and the scale of operations that enable to undertake a systematic observation of the process through which AI raises ambiguity, deniability, persistence and scalability of grey-zone campaigns. Taken together, all of these instances provide empirical evidence to the explanation of how AI can alter the contemporary conflict dynamics, issue of attribution, and deterrence stability, and response in the international governance.

### *A. AI-Based operations in grey-zone in case of Russia-Ukraine.*

The grey-zone warfare that Russia has been waging against Ukraine (the combination of cyber-attacks, information warfare, political influence, and psyche manipulation) is slowly enhanced with AI-powered functionality, before the more conventional form of hostilities are developed in 2022. Machines and automation allowed developing a system of massive disinformation campaigns to shape the domestic and international narratives, hyperpolarize society, and ruin trust in Ukrainian institutions. With the help of AI, people could manipulate social media and control it to promote a certain propaganda, back it with bots, and modify a narrative to the current indicators of the amount of audience engagement. Automation was used in cyber activities to detect vulnerabilities, reconnoitre and launch sustained intrusion attacks into government networks, critical infrastructure and electoral systems. Simultaneously, together with the presence of artificial media and the generation of algorithmic content, it contributed to the mislead, reputational attack, and psychological pressure due to the confusion of the border between the real and fake data. The activities that were enhanced by AI allowed Russia to maintain the persistence of the long-term strategic pressure with no major cost to lose plausible deniability and allowed Ukraine to do the same in the corresponding measures in the political, legislative, or military realms. Thus, it is evident that in the situation of Russia-Ukraine, AI has the potential to sharpen the battle in grey zones because it accelerates the workflow, expands the range of reach of the activity, and involves the war in the non-combat world digital ecosystem.

### *B. AI In the Influence and Information Operations in Democratic Societies.*

Besides the Russia-Ukraine case, the AI has been actively used to carry out the grey-zone influence operation by democratic nations, especially at the time of the electoral process and in times of social unrests. LLMs and content-generation systems encourage people to create persuasive political content, carefully misinformation and emotionally persuasive stories quickly and aimed specifically at a different demographic group in particular. Sentiment analysis and behavioral profiling by an AI can be used by enemies to create awareness of social divisions and disseminate polarizing content and exploit identity-related fault lines in specific target societies. The technologies of deepfakes and synthetic media make it even more difficult to achieve the integrity of information as individuals can successfully operate in the sphere of impersonation of political leaders, and journalists and other individuals and challenge the trust to the democratic institutions and media systems. These actions are usually lesser than the explicit interference, and they are of a compound psychological and political effect. The situation explains how AI will change the power of operations into the scalable, flexible, and sustainable grey-zone instruments that will be able to reshape the political arguments without triggering the usual deterrence instruments.

*C. AI-based Strategic Coercion of Cyber Competition and Economic Competition.*

Another area of AI use is the grey-zone cyber and economic coercion in which non-kinetic strategic coercion can be more effective, extensive, and sustainable by being augmented with automated mechanisms. The machine-learning domain is utilized in the cyber domain to accelerate the vulnerability identification process and to automatically identify the intrusion, malware development, and evasion of protection measures in real-time, which enables to arrange the continuous campaigns of uncontrolled espionage and disruption of the essential infrastructure, monetary, and defense systems. The analytics of AI has the potential to be applied in the economic sphere to manipulate the market, optimize the sanctions, analyze the trade leverage and predictive forecast of a financial crisis in a target state. Such capabilities enable actors to make their economy and digital pressure through coercion that can be denied and without the need to go through an open confrontation. With the introduction of AI into the cyber and economic tools market, states would be able to create long-term strategic pressure, restricting the strength of rivals, confining policy discretion, and increasing the competitive edge on the long-term basis, as they will be operating within the grey-zone industry.

## VI. IMPLICATIONS FOR DETERRENCE, ATTRIBUTION, AND STRATEGIC STABILITY

The fact that AI-enabled grey-zone conflict can cause significant issues with the credibility of deterrence, attribution processes, and long-term strategic stability is a problem because it shifts the theoretical foundations of the theory of International Relations (IR) and the security practice. The traditional deterrence theory that have their roots in the rational actor theory, attribution clarity and the credible retaliation are proving ineffective, in the world that aggressive behavior is denyable, automated, decentralized and legally gray. There is such issue associated with the AI as the attribution problem, which is a paramount problem of IR in that it conceals intent, acceleration of the speed of operations, and invasiveness of the digital environment of civilians, which weakens the ability of the states to attribute responsibility or to respond in an equal measure. This, as per realist perceptions, would tear the signaling of balance of power, because it enables an occurrence of further coercion, without the classical escalation. Systems of liberal institutionalists fail to establish a sense of accountability due to the divided jurisdiction, slow norms making and enforcement in the sphere of cyberspace and informational field. The concept of stability is also more complex in constructivist dynamics since the manipulation of the narrative the AI enables can redefine the perception of threats, legitimacy claims, and identity based conflict framing. Brought in combination these effects enhance the chances of miscalculation, escalation ambiguity, deterrence erosion and strategic instability, which is a means to entrench a security environment, in which the struggle is continuous low intensity competition, rather than discrete high acuity conflict.

TABLE 4
AI IMPLICATIONS FOR DETERRENCE, ATTRIBUTION, AND STRATEGIC STABILITY — AN IR PERSPECTIVE

| Security Dimension | AI-Driven Impact | Relevant IR Theory Lens | Strategic Risk | Implications for Global Stability |
|---|---|---|---|---|
| Deterrence Credibility | Obscures attacker identity and reduces cost of repeated low-level aggression | Realism, Rational Deterrence Theory | Weakens retaliatory signaling and response credibility | Encourages persistent sub-threshold coercion |
| Attribution & Responsibility | Automates operations and masks state involvement through proxies and platforms | Liberal Institutionalism, Legal Norms | Limits legal accountability and diplomatic response | Increases norm erosion and impunity |
| Escalation Control | Compresses decision cycles and increases speed of conflict dynamics | Crisis Stability Theory, Game Theory | Raises risk of miscalculation and unintended escalation | Destabilizes crisis management and escalation ladders |
| Norm & Rule Stability | Exploits regulatory gaps and outpaces | Liberal Institutionalism, | Undermines international legal regimes | Weakens institutional authority and rule- |

| | | | | |
|---|---|---|---|---|
| | international governance frameworks | Global Governance Theory | | based order |
| Perception & Legitimacy | Manipulates narratives, identities, and threat framing | Constructivism, Soft Power Theory | Distorts public opinion and legitimacy judgments | Erodes trust in democratic and multilateral institutions |
| Balance of Power | Lowers entry barriers for smaller states and non-state actors | Structural Realism | Shifts power distribution toward asymmetric actors | Increases volatility in regional power dynamics |
| Arms Race Dynamics | Accelerates AI competition and security dilemma effects | Security Dilemma Theory, Offensive Realism | Intensifies technological arms competition | Heightens long-term instability and arms race pressures |
| Crisis Signaling & Misinterpretation | Generates ambiguous or automated signals lacking clear political intent | Signaling Theory, Strategic Interaction Models | Increases misunderstanding and misperception | Elevates risk of accidental escalation |
| Long-Term Strategic Stability | Embeds persistent low-level competition into daily political systems | Hegemonic Stability Theory | Normalizes chronic geopolitical friction | Sustains prolonged systemic instability |

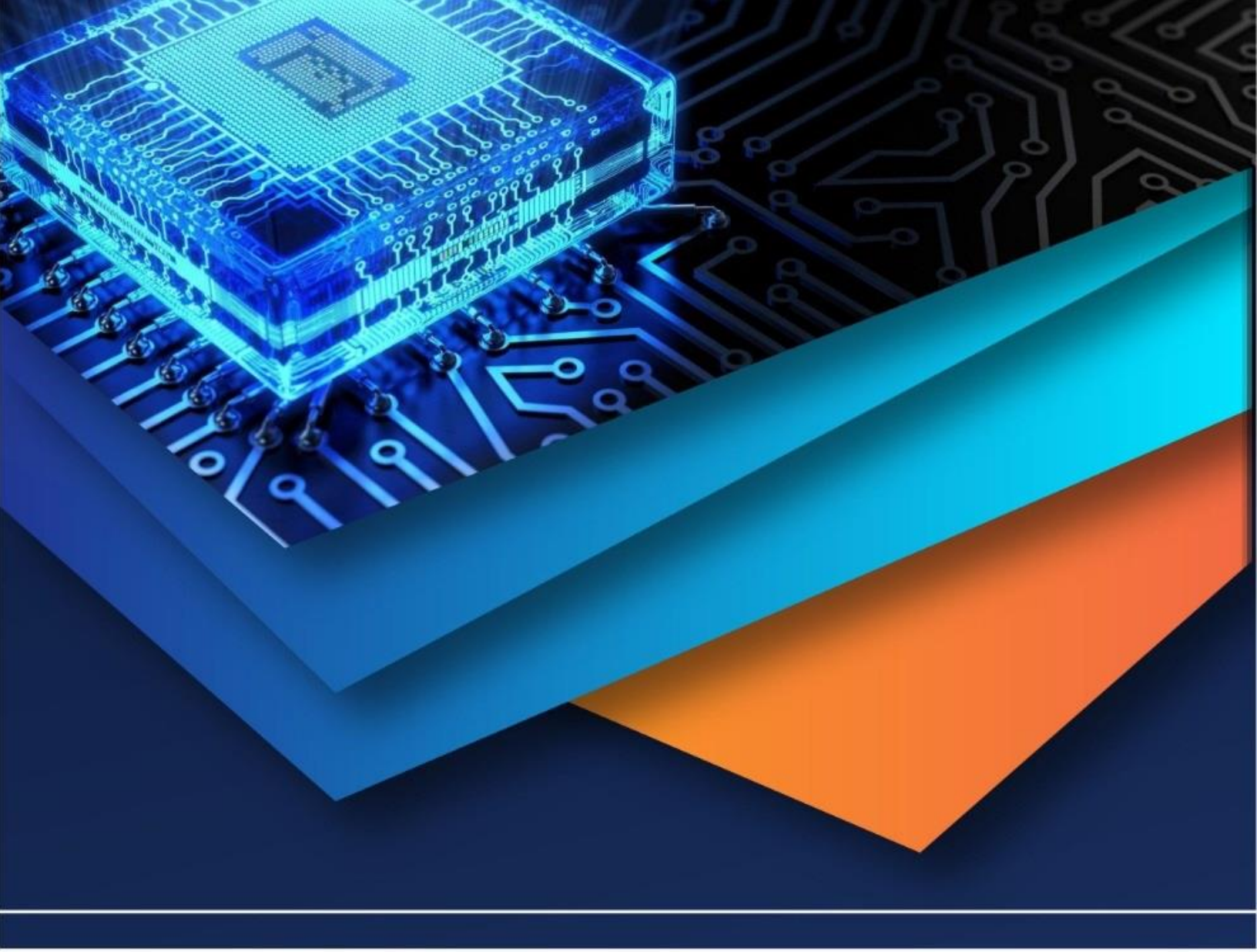
## VII. CONCLUSION

The fact that AI-enabled grey-zone conflict can cause significant issues with the credibility of deterrence, attribution processes, and long-term strategic stability is a problem because it shifts the theoretical foundations of the theory of International Relations (IR) and the security practice. The traditional deterrence theory that have their roots in the rational actor theory, attribution clarity and the credible retaliation are proving ineffective, in the world that aggressive behavior is denyable, automated, decentralized and legally gray. There is such issue associated with the AI as the attribution problem, which is a paramount problem of IR in that it conceals intent, acceleration of the speed of operations, and invasiveness of the digital environment of civilians, which weakens the ability of the states to attribute responsibility or to respond in an equal measure. This, as per realist perceptions, would tear the signaling of balance of power, because it enables an occurrence of further coercion, without the classical escalation. Systems of liberal institutionalists fail to establish a sense of accountability due to the divided jurisdiction, slow norms making and enforcement in the sphere of cyberspace and informational field. The concept of stability is also more complex in constructivist dynamics since the manipulation of the narrative the AI enables can redefine the perception of threats, legitimacy claims, and identity based conflict framing. Brought in combination these effects enhance the chances of miscalculation, escalation ambiguity, deterrence erosion and strategic instability, which is a means to entrench a security environment, in which the struggle is continuous low intensity competition, rather than discrete high acuity conflict.

## REFERENCES

[1] Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars (p. 51). Arlington, VA: Potomac Institute for Policy Studies.
[2] Mazarr, M. J. (2015). Mastering the gray zone: understanding a changing era of conflict.
[3] Kumar, N., & Patel, N. M. (2025). Social engineering attack in the era of generative AI. International Journal for Research in Applied Science and Engineering Technology, 13(1), 1737-1747.
[4] Mearsheimer, J. J. (2025). War and international politics. International Security, 49(4), 7-36.
[5] Keohane, R. O., & Nye Jr, J. S. (1973). Power and interdependence. Survival, 15(4), 158-165.
[6] Wendt, A. (1999). Social theory of international politics (Vol. 67). Cambridge university press.
[7] Kello, L. (2017). The virtual weapon and international order. Yale University Press.

[8] Kumar, N., Parekha, C., & Sheth, R. (2025). Exploring 6G Wireless Networks: A Comprehensive Analysis. Virtual Reality and Augmented Reality with 6G Communication, 51-88.
[9] Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. WW Norton & Company.
[10] Hopgood, A. A. (2021). Intelligent systems for engineers and scientists: a practical guide to artificial intelligence. CRC press.
[11] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.
[12] Loik, R. (2025). EU–NATO Cooperation and Perspectives on Countering Hybrid Threats. In Russian Influence Operations and the War in Ukraine: Hybrid Warfare and Disinformation Campaigns (pp. 207-234). Cham: Springer Nature Switzerland.
[13] Yousefi, M., & Habibi, R. (2022). Analysis of US Strategic Documents (National Security Strategy, National Defense Strategy, and National Military Strategy). Journal Strategic Studies of Public Policy, 11(41).
[14] Fridman, O. (2018). Russian" hybrid warfare": Resurgence and politicization. Oxford University Press.
[15] Kumar, N., Deshkar, D., & Patel, N. (2025, November). Fine-Tuning Language Models for Social Engineering: A Technical Feasibility Study. In 2025 IEEE 7th International Conference on Computing, Communication and Automation (ICCCA) (pp. 1-6). IEEE.
[16] Deshkar, D. (2025). QUANTITATIVE AND COMPUTATIONAL MATHEMATICAL ANALYSIS OF GEN-AI-FACILITATED SOCIAL ENGINEERING THREATS. International Journal of Applied Mathematics, 38(10s), 2159-2179.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY