ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Artificial Intelligence and Terrorist Groups in the Middle East: A Strategic Analysis of Capabilities and Security Implications from the Perspective of Offensive Realism

Mojtaba. Sadeqi[1], Ehsan. Razani[2*], Mohammad Fazel. Sadri[3]

[1] Ph.D. Student, Department of International Relations, Sha.C., Islamic Azad University, Shahrud, Iran
[2] Department of International Relations, Sha.C., Islamic Azad University, Shahrud, Iran
[3] Department of Political Science, Sha.C., Islamic Azad University, Shahrud, Iran

*** Corresponding author email address**: Drrazani@iau.ac.ir

Received: 2026-06-07 **Revised:** 2026-08-27 **Accepted:** 2026-09-02 **Initial Publish:** 2026-09-03 **Final Publish:** 2027-09-01

The emergence of artificial intelligence (AI), alongside transformations in the patterns of power production and exercise, has created new capabilities for both state and non-state actors within the international security environment. Given their historical adaptability to digital technologies, terrorist groups may also potentially exploit certain AI capabilities in areas such as cognitive warfare, content generation and dissemination, intelligence analysis, cyber operations, communications, and recruitment. The present study aims to analyze the strategic capabilities and implications of artificial intelligence for terrorist groups in the Middle East and to explain these developments from the perspective of offensive realism. In terms of purpose, the study is applied, and in terms of methodology, it adopts a descriptive-analytical approach based on documentary and library research. The findings indicate that, rather than creating material parity between terrorist groups and states, artificial intelligence can function as a force multiplier for these groups' intelligence, cognitive, communication, and organizational capabilities. Moreover, the utilization of AI capabilities may reduce certain technological constraints, enhance the capacity for survival and influence, intensify strategic ambiguity, and alter the cost-effectiveness ratio of operations, thereby facilitating a form of asymmetric balancing in the non-material dimensions of power. Nevertheless, the available evidence regarding the practical and systematic use of certain advanced AI capabilities by terrorist groups remains limited, and a distinction must therefore be drawn among documented applications, potential capabilities, and future threats. Accordingly, artificial intelligence can be regarded as one of the factors contributing to the transformation of the Middle Eastern security environment. While preserving the material superiority of states, it simultaneously creates new arenas for technological, informational, and cognitive competition.

Keywords: *artificial intelligence, terrorism, Middle East, offensive realism*

How to cite this article:
Sadeqi, M., Razani, E., & Sadri, M. F. (2027). Artificial Intelligence and Terrorist Groups in the Middle East: A Strategic Analysis of Capabilities and Security Implications from the Perspective of Offensive Realism. *Interdisciplinary Studies in Society, Law, and Politics, 6*(5), 1-12. https://doi.org/10.61838/kman.isslp.568

1. Introduction

Rapid technological developments in recent decades have fundamentally transformed the nature of power, security, and threat within the international system. The emergence of technologies such as artificial intelligence (AI), big data, machine learning, autonomous systems, and generative artificial intelligence has shifted many processes related to information collection and analysis, communications, content generation, data processing, and decision-

making from traditional patterns to digital and algorithmic environments (Basiri & Mohseni, 2023; Bazarkina, 2023; Davis, 2021). Under such conditions, technology is no longer merely an instrument serving the political, economic, and military power of states; rather, it has become one of the factors shaping power capabilities and redefining patterns of competition and threat in the security environment. This transformation becomes even more significant when access to certain capabilities of emerging technologies is no longer monopolized by states and major military establishments, allowing non-state actors to exploit some of these capabilities as well (Briefs, 2026; Shiroudi et al., 2020; Vashishtha, 2023).

Among non-state actors, terrorist groups are of particular significance because the experience of the past two decades has demonstrated their considerable capacity to adapt to technological developments and transfer parts of their activities from the physical environment to the digital sphere. Even before the emergence of artificial intelligence, the Internet, social networks, and messaging platforms had become tools for propaganda, ideological dissemination, recruitment, communication with supporters, network organization, and the expansion of the transnational activities of terrorist groups (Djoric & Milosevic, 2021; Ganaie, 2025; Gholami, 2021). The introduction of artificial intelligence into this environment does not necessarily imply the emergence of an entirely new form of terrorism; rather, it can reinforce the existing capabilities of terrorist groups by increasing speed, scale, accuracy, personalization, and automation. Generative artificial intelligence can facilitate the production of text, images, audio, and video; data-analysis algorithms can process large volumes of information within short periods; translation tools and multilingual content-generation systems can expand the communicative reach of extremist groups; and automated systems can facilitate parts of their communication and propaganda processes (Hosseini et al., 2025; Juelich, 2026; Olech, 2026). Recent studies have also emphasized that generative artificial intelligence and language models may be misused in areas such as propaganda, radicalization, recruitment, and the dissemination of violent narratives.

From this perspective, the relationship between terrorism and artificial intelligence is not merely a technical or technological issue; rather, it has become an issue of power and international security. The central question is how artificial intelligence can alter the capacity of a terrorist actor to exert influence and how such changes in capacity may affect the surrounding security environment. Terrorist groups are not comparable with states in terms of economic, military, intelligence, or infrastructural resources; nevertheless, certain digital technologies can enable them to generate greater impact with more limited resources in areas such as information production and dissemination, propaganda, cognitive operations, communications, and data processing (Houser & Dong, 2025; Vashishtha, 2023). Therefore, the significance of artificial intelligence for terrorism should not be reduced to the claim that it eliminates the material superiority of states; rather, it should be understood as a force multiplier for certain existing terrorist capabilities and as a factor capable of reducing some of the traditional constraints confronting non-state actors.

This transformation is of even greater significance in the Middle East. The persistence of armed conflicts, the presence of armed non-state groups, weak or fragile governance structures in some countries, competition among regional and extra-regional powers, identity and political crises, and the expansion of communication infrastructures have created a multilayered and complex environment for the evolution of security threats (Bashiri, 2022; Elyaari, 2024; Ezeamalu, 2026; Soliman, 2026).

In such an environment, terrorist groups and violent extremist networks can adapt new technologies to their own operational and communication conditions. The experience of groups such as ISIS and al-Qaeda has demonstrated that cyberspace can become an arena for the reproduction of transnational networks, the dissemination of ideological narratives, audience recruitment, and communication with supporters (Bakhshi-Sheikh-Ahmad, 2015; Ezeamalu, 2026; Ford, 2026). In the emerging environment, artificial intelligence can make some of these activities faster, broader in scope, and more personalized, thereby rendering the boundary between the physical and digital activities of terrorist groups more fluid than before.

The strategic significance of this transformation can also be examined in terms of changes in the sources and forms of power. In traditional conceptions of power in international relations, military, economic, and

territorial capabilities are regarded as among the most important sources of power; however, the transformation of the digital environment has also converted informational and cognitive capabilities into important sources of influence. The ability to collect and process information, generate and disseminate narratives, influence public perceptions, analyze audience behavior, and create ambiguity within the information environment can constitute part of an actor's strategic power capabilities (Bazarkina, 2023; Li et al., 2026; Muperi, 2026). Artificial intelligence should therefore not be regarded as a substitute for material power; rather, it should be understood as a factor that alters the manner in which informational and cognitive resources are converted into political and security influence. This issue is particularly important for terrorist groups because, given their limited material resources, they have consistently sought methods of achieving greater impact at lower cost.

Under such conditions, offensive realism can provide an important framework for analyzing part of this transformation. Offensive realism, particularly as formulated by John Mearsheimer, is based on the propositions that the international system is anarchic, states can never be completely certain about one another's intentions, survival is their fundamental objective, and actors in an insecure environment rationally seek to increase their power and relative position (Barzegar, 2009; Mearsheimer, 2001, 2012). Within this framework, anarchy, offensive capabilities, uncertainty regarding the intentions of others, the importance of survival, and actor rationality constitute the theory's fundamental assumptions. From this perspective, technological transformation becomes theoretically significant when it can affect the distribution of capabilities, calculations of power, levels of vulnerability, and degrees of uncertainty in the security environment.

Nevertheless, applying offensive realism to the analysis of terrorist groups entails an important theoretical limitation. Offensive realism is fundamentally a state-centric theory, and terrorist groups cannot be considered equivalent to states or great powers in legal, structural, or material-capability terms. Accordingly, the present study does not claim a direct extension of offensive realism to terrorist groups; rather, it employs selected concepts from this theory—including survival, power, competition, self-help, uncertainty, and the enhancement of influence capabilities—as an analytical lens for examining the behavior and technological capacities of terrorist actors.

This approach is consistent with recent studies that have sought to incorporate the cognitive, informational, and cultural dimensions of power into realist analyses (Li et al., 2026; Muperi, 2026). Accordingly, the terrorist group in the present study is not regarded as a "state," but rather as a non-state actor that, within a highly contentious security environment, may employ certain emerging technologies to enhance its capacity for survival, influence, and impact.

Within this framework, the concept of asymmetric balancing assumes particular importance. Asymmetric balancing in the present study does not imply material parity between terrorist groups and states; rather, it refers to a situation in which a weaker actor can use technologies such as artificial intelligence to reduce some of its traditional constraints in the fields of information, communications, propaganda, and cognitive operations. In other words, artificial intelligence may enable terrorist groups to increase their capacity for influence with more limited resources and to narrow part of the gap between their material capabilities and those of states in non-material domains (Houser & Dong, 2025; Shiroudi et al., 2020; Vashishtha, 2023). Therefore, the central issue is not the elimination of states' material superiority, but rather changes in certain relationships among cost, speed, and influence capacity between state and non-state actors.

Another important dimension of this issue concerns the impact of artificial intelligence on strategic ambiguity and uncertainty. Synthetic content generation, identity falsification, the dissemination of misleading information, automation of certain digital activities, and difficulties in identifying the origin of some activities can complicate the threat-assessment process for states (Bazarkina, 2023; Djoric & Milosevic, 2021; Razmkhah, 2024). Under such conditions, states may face greater difficulty in identifying the source of a threat, assessing an actor's actual capabilities, and predicting its future behavior. This issue is related to the concept of uncertainty in offensive realism, because the more difficult it becomes for states to assess the capabilities and intentions of opposing actors, the greater the likelihood of precautionary calculations, security

competition, and increased efforts to reduce vulnerability.

At the same time, examining the relationship between artificial intelligence and terrorism requires conceptual and methodological caution. Not every use of digital technology can be considered an application of artificial intelligence, nor does every technological capability necessarily imply the actual and systematic use of that technology by terrorist groups (Houser & Dong, 2025). Accordingly, the present study distinguishes among documented applications of artificial intelligence, the potential capacity for its utilization, and possible future scenarios. This distinction is particularly important with respect to advanced cyber operations, algorithmic targeting, and autonomous systems, because some claims in these areas are based on technological potential or future projections rather than definitive evidence of operational use by terrorist groups. Such conceptual caution is essential for avoiding threat inflation and maintaining the scientific validity of the analysis.

From this perspective, the research problem is not merely whether terrorist groups use artificial intelligence; rather, the more fundamental question is how artificial intelligence changes the capabilities of terrorism and what consequences these changes have for power, survival, strategic ambiguity, and the balance of threats in the Middle East. Answering this question requires establishing a connection among three bodies of literature that have often been examined separately: first, the literature on artificial intelligence and emerging technologies; second, the literature on terrorism and regional security; and third, the literature on offensive realism and competition for power. The present study seeks to integrate these three domains within a unified analytical framework. In this regard, the applications and potential uses of artificial intelligence by terrorist groups can be examined in such areas as cognitive warfare and perception manipulation, intelligence analysis and support for reconnaissance, financial activities and digital networks, cyber operations and propaganda, automated communications, and recruitment. The significance of these areas is not limited to their technical capabilities; rather, each may reduce some of the traditional constraints faced by terrorist groups and enhance their capacity for survival, influence, communication, narrative production, and the imposition of costs on states. Conversely, the same technologies can also be employed by states and security institutions for the detection, prevention, and countering of terrorism. Artificial intelligence should therefore be regarded as part of a two-sided technological, informational, and cognitive competition rather than as a technology available exclusively to terrorist groups (Hosseini et al., 2025; Razmkhah, 2024). Despite the growth of research on artificial intelligence, terrorism, and cybersecurity, a substantial gap remains in studies that simultaneously examine all three domains. Some existing studies have focused on the technical capabilities of artificial intelligence or its use by states; others have addressed the role of digital technologies in propaganda, radicalization, and recruitment; while studies of offensive realism have predominantly examined the behavior of states, particularly great powers (Davis, 2021; Fong, 2026; Ganaie, 2025; Olech, 2026). Within the Persian-language literature, although studies have examined artificial intelligence and the future of terrorist attacks, cyberterrorism, the media behavior of terrorism, and offensive realism (Bashiri, 2022; Gholami, 2021; Hosseini et al., 2025; Shiroudi et al., 2020), the systematic relationship among AI capabilities, changes in the capacities of terrorist groups, and their implications for the balance of threats in the Middle East from the perspective of offensive realism still requires further investigation.

Accordingly, focusing on the Middle East, the present study seeks to identify the applications and potential uses of artificial intelligence by terrorist groups and to examine the strategic implications of this transformation for the regional security environment. The principal research question is: How can the applications and potential use of artificial intelligence by terrorist groups in the Middle East be explained, and what implications does this transformation have for power, survival, strategic ambiguity, and the balance of regional threats from the perspective of offensive realism? The central proposition of the study is that artificial intelligence, without eliminating the material superiority of states, can increase the informational, cognitive, and communicative capabilities of terrorist groups, reduce some of their technological constraints, and complicate the processes of threat identification and attribution, thereby facilitating asymmetric balancing, increasing strategic ambiguity, and transforming the security

environment of the Middle East. The present study employs offensive realism as an analytical lens for interpreting certain dimensions of the strategic behavior of terrorist groups, rather than as a theory that fully explains these actors within its state-centric framework. The importance of the study lies in examining artificial intelligence not merely as a new technology and terrorism not merely as a traditional security threat, but at the intersection of technology, power, and strategic competition. From this perspective, the article does not seek to exaggerate the technological capabilities of terrorist groups; rather, it seeks to understand how access to certain AI capabilities can alter the form, speed, scale, and cost of terrorist activities and thereby transform certain aspects of the Middle Eastern security equation. Such an approach, while acknowledging the theoretical limitations of offensive realism, can provide a basis for reconsidering the concepts of power, threat, and competition in the digital security environment.

2. Research Method

The present study is applied in terms of purpose and descriptive-analytical in terms of nature and methodology, and it was conducted using documentary and library research methods. The objective of the study is to identify and analyze the areas in which terrorist groups in the Middle East may use or potentially exploit artificial intelligence and to examine the strategic implications of such developments for regional security and the balance of threats from the perspective of offensive realism. Given the nature of the study, no statistical testing or quantitative modeling was intended; rather, the available information was collected, classified, and analyzed.

The theoretical framework of the study is based on offensive realism, and concepts such as power, survival, anarchy, uncertainty, strategic ambiguity, and enhanced influence capacity form the basis of the analysis. Research data were collected and analyzed through the examination of books, scholarly articles, theses and dissertations, research and official reports, documents issued by international organizations, and credible news sources, using keywords such as artificial intelligence and terrorism, artificial intelligence and cognitive warfare, terrorism and cybersecurity, armed non-state actors, terrorism in the Middle East, and offensive realism. Information concerning the application of artificial intelligence was classified into five principal domains: cognitive warfare and perception manipulation; reconnaissance and intelligence analysis; financing and digital financial networks; cyber operations and propaganda; and automated communications and recruitment. These domains were subsequently examined in relation to the concepts of offensive realism. In addition, to enhance analytical precision, distinctions were drawn among documented applications, potential capabilities, and possible future threats. Finally, the relationship between AI applications and components such as power, survival, asymmetric balancing, strategic ambiguity, and the transformation of the Middle Eastern security environment was analyzed, and their implications for the regional security order were examined.

3. Research Findings

The examination and analysis of documents, scientific studies, and reports concerning the relationship between artificial intelligence and terrorism indicate that the introduction of intelligent technologies into the security environment of the Middle East has not so much created an entirely new form of terrorism as strengthened, accelerated, and increased the scalability of certain existing terrorist capabilities. This transformation can be analyzed through the relationship among the three principal components of the study: terrorism, artificial intelligence, and the logic of power in offensive realism.

Within this framework, artificial intelligence can function as a force multiplier by increasing the cognitive, informational, communicative, and organizational capabilities of terrorist groups without completely eliminating the material superiority of states (Olech, 2026; Shiroudi et al., 2020; Vashishtha, 2023).

The first identified domain is cognitive warfare and perception manipulation. The literature indicates that generative artificial intelligence can increase the capacity for the rapid and large-scale production of text, images, audio, and video, thereby strengthening the propaganda and communication tools available to extremist and terrorist groups (Bazarkina, 2023; Ganaie, 2025; Hosseini et al., 2025). The significance of this issue for the relationship between artificial intelligence and terrorism lies in the fact that the power of terrorist groups is no longer confined solely to their capacity to

perpetrate physical violence; rather, the ability to influence audience perceptions, produce narratives, and create psychological effects has also become part of their capacity for influence. Under these conditions, artificial intelligence can reduce the time between content production and dissemination and facilitate the generation of content tailored to different audiences (Juelich, 2026; Olech, 2026).

In relation to offensive realism, this transformation is particularly significant because power in this context does not appear solely in the form of military and economic resources; rather, part of an actor's power capacity is manifested in its ability to influence the perceptions and calculations of a rival actor. Artificial intelligence may therefore enable terrorist groups to affect the security environment in a non-material domain without possessing material resources comparable to those of states.

Such a situation may be characterized as a form of asymmetric balancing in the cognitive and informational domains, a concept employed in the present study to explain the relative reduction of certain power constraints affecting non-state actors (Li et al., 2026; Mearsheimer, 2001).

The second domain concerns intelligence analysis and support for target identification. Existing studies indicate that data-analysis tools, image processing, pattern recognition, and open-source intelligence analysis can increase the capacity of non-state actors to process large volumes of information (Houser & Dong, 2025; Vashishtha, 2023). An important point in this regard is that not every use of digital data should be considered an application of artificial intelligence. Nevertheless, technological development trends suggest that intelligent tools may in the future increase the capacity of non-state actors to process information and identify patterns relevant to their operational environments.

From the perspective of terrorism, such a capability can increase the capacity to analyze the environment, identify opportunities, and reduce some of the information asymmetry between non-state groups and states. From the perspective of offensive realism, its significance can be explained in relation to the concepts of relative power and uncertainty: the greater an actor's capacity to collect and process information, the greater its ability to make strategic decisions and adapt to the security environment. Nevertheless, the existing evidence regarding the actual and systematic use of advanced AI systems by terrorist groups in this domain remains limited; accordingly, documented use must be distinguished from potential capacity.

The third domain concerns digital financial networks and the use of intelligent capabilities in resource management. Studies addressing terrorism and technology indicate that the digitalization of financial systems, cryptocurrencies, and decentralized networks has created a new environment for financing and resource transfers (Houser & Dong, 2025). Nevertheless, evidence concerning the direct use of advanced artificial intelligence algorithms by terrorist groups to manage and conceal financial resources remains limited. Accordingly, this domain should be discussed primarily in terms of technological capacity and possibility rather than as an established and widespread practice.

The significance of this domain in relation to offensive realism lies in the fact that the survival and continuity of any actor depend on access to resources. Technologies capable of reducing transaction, communication, and resource-management costs may therefore potentially enhance the organizational survival capacity of terrorist groups. In this sense, artificial intelligence can be analyzed not as an independent source of power but as a multiplier of the efficiency of existing resources. The fourth domain concerns cyber operations and adaptive capabilities in the digital sphere. The literature indicates that artificial intelligence performs two opposing functions in cybersecurity: on the one hand, it can increase the capacity to detect and counter attacks; on the other hand, if misused, it can contribute to increasing the complexity and scale of certain threats (Khoumich et al., 2026; Macdonald et al., 2024). Nevertheless, claims concerning the widespread and demonstrated use of fully autonomous and adaptive systems by terrorist groups for cyber operations require more precise evidence.

From the perspective of offensive realism, the significance of cyber operations lies in their capacity to generate strategic ambiguity. In the digital environment, identifying the source of an attack, determining an actor's level of capability, and assessing its actual objective may become more difficult. This situation is related to the logic of uncertainty in offensive realism, because greater ambiguity concerning actors'

capabilities and intentions can complicate the security calculations of states (Fong, 2026; Mearsheimer, 2001). The fifth domain concerns propaganda, automated communications, and the recruitment of members and supporters. Compared with certain more advanced applications of artificial intelligence, this domain is supported by a larger body of evidence in the existing literature. Even before the emergence of artificial intelligence, terrorist groups and extremist movements used the Internet and social media for ideological dissemination, propaganda, audience engagement, and recruitment (Djoric & Milosevic, 2021; Ganaie, 2025; Gholami, 2021). The introduction of AI tools can strengthen these capabilities through multilingual content generation, message personalization, audience analysis, and partial automation of communications.

This transformation indicates that the relationship between artificial intelligence and terrorism is not merely a relationship between technology and violence, but also one between technology and socio-cognitive power. A terrorist group can use technology to expand its reach, maintain communication with audiences, and sustain its narrative. From this perspective, artificial intelligence becomes an instrument for converting limited resources into broader communicative capacity (Ganaie, 2025; Olech, 2026).

At a more general level, the examination of the five domains discussed above indicates that artificial intelligence primarily functions as a force multiplier in contemporary terrorism. This technology does not independently neutralize the material power of states, but it can increase the influence capacity of terrorist groups in certain non-material domains, including information, communications, propaganda, data analysis, and cognitive operations. Accordingly, the relationship between state power and the technological capabilities of terrorist groups should be understood as asymmetric and complementary rather than as a relationship based on equality of power (Houser & Dong, 2025; Vashishtha, 2023). Another finding concerns the relationship among artificial intelligence, terrorism, and strategic ambiguity. The increased production of synthetic content, the possibility of identity falsification, and the difficulty of distinguishing authentic from fabricated content can complicate the security decision-making environment (Bazarkina, 2023; Turner, 2026). Under such conditions, states are not confronted merely with the problem of countering an attack; they must also make judgments regarding the credibility of information, the origin of a threat, and the actor's actual level of capability. Artificial intelligence can therefore become one of the factors increasing uncertainty within the security environment. Another finding concerns the enhanced survival capacity and network adaptability of terrorist groups. Terrorist groups operating in unstable Middle Eastern environments face military, security, intelligence, and financial pressures. The use of digital technologies can reduce some of their communication and organizational costs and enable the reconstruction or continuation of communication networks (Djoric & Milosevic, 2021; Soliman, 2026). From the perspective of offensive realism, this issue is related to the importance of survival, because any factor that increases an actor's ability to persist within an insecure environment is strategically significant.

At the regional level, the evidence also indicates that the distinctive security structure of the Middle East provides a conducive environment for the interaction of technology, terrorism, and power competition. The persistence of armed conflicts, the presence of non-state actors, competition among regional and extra-regional powers, weak governance in certain areas, and social and political divisions cause emerging technologies to interact with existing threats (Bashiri, 2022; Ezeamalu, 2026; Soliman, 2026). Accordingly, the actual or potential use of artificial intelligence by terrorist groups cannot be examined independently of the geopolitical structure of the Middle East.

4. Discussion and Conclusion

The introduction of artificial intelligence into the sphere of terrorism does not merely represent the addition of a new technology to the range of tools employed by violent actors; rather, it indicates an important transformation in the production, transmission, and exercise of power within the contemporary security environment. In the Middle East, this transformation assumes greater significance because of persistent conflicts, the presence of armed non-state actors, regional and extra-regional rivalries, and the relative fragility of certain security structures. Within such an environment, artificial intelligence can strengthen the communicative, informational, cognitive, and organizational capabilities of terrorist groups and reduce some of the constraints

arising from their limited material resources. From this perspective, the central concern of the present study is not the replacement of military power by technological power, but rather the manner in which technology may be transformed into a force multiplier and a source of threat capacity for non-state actors.

From the perspective of offensive realism, the significance of this transformation can be explained through concepts such as survival, power, competition, and uncertainty. Offensive realism assumes that actors operating in an anarchic environment must continuously attend to power and influence capabilities in order to preserve their survival and improve their position (Mearsheimer, 2001). Although this theory was fundamentally developed to explain state behavior, a limited and analytical application of its concepts can also be useful for understanding terrorist groups, provided that such groups are not treated as equivalent to states. Within this framework, terrorist groups can be regarded as actors that exploit available technological opportunities in insecure environments in order to survive, preserve their networks, increase their influence, and impose costs on their adversaries.

From this perspective, the most important issue is that artificial intelligence can alter the means through which power is acquired and exercised. The power of terrorist groups does not necessarily entail greater military capacity or territorial control; it may also be exercised through the ability to influence perceptions, information, public opinion, and the security calculations of states. This interpretation is consistent with research demonstrating that AI technologies can be exploited for radicalization, recruitment, and extremist propaganda and can increase the capacity to generate personalized and targeted content (Ganaie, 2025). Thus, what is significant in this context is the transformation of technology into influence capacity—a capacity that can reduce some of the traditional constraints faced by terrorist groups without generating material parity with states.

This conclusion is also consistent with studies emphasizing the capacity of artificial intelligence to increase the speed, scale, and effectiveness of the communicative, propagandistic, and cognitive activities of extremist groups (Ganaie, 2025; Olech, 2026; Vashishtha, 2023). In the same vein, systematic reviews have shown that terrorist organizations have historically demonstrated an ability to adapt to emerging technologies and that the convergence of artificial intelligence and terrorism may create new capabilities for such groups (Houser & Dong, 2025). The present study, however, takes the analysis a step further by examining the issue not merely in terms of technological capability, but by linking it to the logic of power and asymmetric balancing within the framework of offensive realism.

In this context, the concept of asymmetric balancing assumes particular importance. Because terrorist groups lack the economic, military, and institutional resources of states, they are unable to compete conventionally with them; however, technology can allow them to reduce part of this gap in areas such as information, communications, propaganda, and cognitive operations. Accordingly, asymmetric balancing in the present study does not refer to the creation of material equilibrium, but rather to an increased capacity to impose costs and disrupt an adversary's calculations through the use of more limited technological resources. This interpretation is consistent with findings in the literature on technology-enabled terrorism as well as research on security competition within the framework of offensive realism.

Another important dimension of this transformation is the increase in strategic ambiguity. Artificial intelligence can make it more difficult to distinguish authentic from synthetic content, identify the origin of certain digital activities, and accurately assess actors' capabilities. In this respect, technology not only increases the operational capabilities of terrorist groups but may also intensify uncertainty within the security environment. This issue is directly related to one of the fundamental assumptions of offensive realism: uncertainty regarding the intentions and capabilities of other actors. Under such conditions, states may encounter greater difficulty in determining the source of a threat, evaluating its actual capability, and selecting an appropriate response. This interpretation is consistent with studies addressing the capacity of artificial intelligence to generate misleading content and influence perceptions (Bazarkina, 2023; Olech, 2026). Research examining the relationship among cognitive warfare, the logic of power, and offensive realism is also noteworthy in this regard, as it demonstrates that power competition in the emerging environment is not confined to the material

domain and that informational and cognitive operations can likewise serve the logic of power (Li et al., 2026).

On the other hand, the findings indicate that artificial intelligence can also affect the concept of survival for terrorist groups. Terrorist organizations operating in highly contested security environments face continuous military, intelligence, and financial pressures. Under such conditions, networked communication, content production, intelligence analysis, and the maintenance of contact with supporters can contribute to the continuity of certain organizational capabilities. Technology may therefore be used not necessarily to create a more powerful organization, but to make the organization more adaptive and resilient. This interpretation is consistent with studies emphasizing the capacity of terrorist organizations to adapt to technological developments.

In this context, research on AI-enabled radicalization is particularly important because it indicates that artificial intelligence can personalize processes of radicalization, recruitment, and propaganda and tailor generated content to audience characteristics (Ganaie, 2025). This finding is consistent with the present study's conclusion regarding the transformation of terrorist power from purely physical power toward cognitive and communicative power. Indeed, a terrorist group does not necessarily require extensive territorial control to exert influence; rather, control over attention, narrative, and perception can function as emerging sources of influence.

From this perspective, the concept of power in the Middle Eastern security environment is expanding. Material power remains the foundation of state power, but data, information, analytical capability, processing speed, and the capacity to manage perceptions have also become important sources of power. Artificial intelligence connects these resources and enables large volumes of data to be transformed into usable content. Technological transformation therefore does not eliminate the traditional logic of power; instead, it expands the range of resources and instruments through which power can be exercised. This interpretation is also consistent with the Persian-language studies used in the present research. For example, research has emphasized the capacity of artificial intelligence to generate new forms of terrorist threats (Shiroudi et al., 2020), while another study has highlighted the potential of artificial intelligence for identifying and predicting threats, countering extremism, and managing intelligence operations (Hosseini et al., 2025). The distinction of the present study lies in moving beyond the level of technological application and analyzing these developments within the framework of power competition and threat balancing in the regional security environment. Furthermore, the findings are consistent with the important methodological observation that not every form of digital technology should automatically be equated with the operational use of artificial intelligence by terrorist groups (Houser & Dong, 2025). This distinction is methodologically important because some existing claims regarding terrorist use of artificial intelligence remain at the level of potential capability or future scenarios. Scientific analysis must therefore distinguish among documented applications, potential capacities, and possible future threats. This distinction constitutes one of the strengths of the present approach. The present study does not seek to exaggerate AI capabilities or portray terrorist groups as technologically equivalent to states. On the contrary, the findings indicate that states retain their material superiority, although technology can alter the relationship between resources and influence in certain specific domains. In other words, artificial intelligence may change the balance of influence capacity in particular areas more than it changes the overall balance of power. At the level of regional security, this transformation may also increase the security costs incurred by states. When states confront larger volumes of fabricated content, cognitive operations, automated activities, and technology-enabled threats, they are compelled to devote greater resources to monitoring, analysis, verification, and cyber defense. Under such circumstances, even an actor with limited resources may generate relatively high costs for an adversary, thereby creating an asymmetry between cost and effect. This dynamic is compatible with the logic of power competition in offensive realism because the significance of an instrument depends not only on the quantity of power it generates but also on its capacity to alter the calculations and costs of an adversary.

From a policy perspective, these findings demonstrate that counterterrorism in the age of artificial intelligence cannot rely exclusively on military power. Military capability remains fundamentally important, but it must

be complemented by informational, cyber, cognitive, media, and technological capacities. To preserve their superiority in the emerging security environment, states require the ability to rapidly identify threats, analyze data, detect synthetic content, protect information infrastructures, and manage the cognitive information environment of society. At the theoretical level, the findings indicate that offensive realism retains explanatory value for concepts such as survival, power, competition, uncertainty, and attempts to improve strategic position; however, the emergence of artificial intelligence and non-state actors also highlights the limitations of the theory's state-centric orientation. The central issue is therefore not that the logic of power has disappeared in the age of artificial intelligence, but rather that the instruments, resources, and arenas through which power is exercised have changed. From this perspective, the present findings are also consistent with studies emphasizing both the continuing importance of the logic of power and the need to incorporate the cognitive and cultural dimensions of strategic behavior (Fong, 2026; Muperi, 2026). Accordingly, the findings can be situated within a body of literature seeking to adapt realist analysis to transformations in the contemporary strategic environment, with the distinction that the present study focuses specifically on terrorism, artificial intelligence, and Middle Eastern security.

5. Conclusion

The overall findings indicate that artificial intelligence is becoming one of the factors influencing the transformation of the operational environment of terrorism in the Middle East; nevertheless, it has not replaced material and military power. The strategic significance of artificial intelligence lies in its capacity to strengthen the existing cognitive, informational, communicative, and organizational capabilities of terrorist groups and to increase their influence through greater speed, scale, and flexibility. In the relationship among terrorism, artificial intelligence, and offensive realism, the underlying logic remains one of survival and the enhancement of influence capacity within an insecure environment, although the means of pursuing these objectives have changed. Because terrorist groups lack the material power possessed by states, they cannot balance against them through conventional military competition; technology can therefore facilitate a form of asymmetric balancing in cognitive, informational, and technological domains. Accordingly, the principal theoretical conclusion of the study is that artificial intelligence should be understood as a force multiplier for non-state actors rather than as a substitute for material power. In certain domains, this technology can narrow the gap between limited resources and broad influence and can affect state calculations by increasing strategic ambiguity, complicating the attribution of threats, and raising security costs. Consequently, security in the Middle East is becoming increasingly hybrid in the age of artificial intelligence. The boundaries among military security, cybersecurity, information security, and cognitive security are becoming less distinct, and effective counterterrorism requires an integrated approach encompassing all of these domains. Under such conditions, maintaining state superiority cannot be achieved solely through increased military power; it also requires the simultaneous strengthening of informational, technological, cyber, and cognitive capacities. From a theoretical perspective, offensive realism remains useful for explaining the logic of power and survival, but its application to the age of artificial intelligence requires greater attention to non-material sources of power. Data, information, processing capability, cognitive power, and algorithmic capacity can therefore be considered alongside traditional sources of power. The present study thus demonstrates that the relationship between terrorism and artificial intelligence cannot be regarded merely as a technological issue; rather, it forms part of a broader transformation in the sources of power, modes of competition, and threat balancing within the regional security environment of the Middle East. Future research should distinguish actual and documented terrorist use of artificial intelligence from potential capabilities and future scenarios and should examine more precisely the effects of this technology on deterrence, threat balancing, cognitive warfare, and competition between states and non-state actors. This research trajectory can contribute to the development of theoretical literature on the relationship among power, technology, terrorism, and offensive realism in the emerging security environment.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Bakhshi-Sheikh-Ahmad, M. (2015). *The Ideology of Takfiri-Wahhabi Terrorist Groups from Al-Qaeda to ISIS*. Jahad Daneshgahi, Publications Organization.

Barzegar, K. (2009). Iran's Foreign Policy from the Perspective of Offensive and Defensive Realism. *Foreign Relations*(1), 113-154.

Bashiri, Q. (2022). *Factors of Emergence of Terrorist Groups and Their Impact on Security*. Arshadan Educational and Authoring Institute.

Basiri, M. A., & Mohseni, M. B. (2023). *The Concept of the Evolution of Artificial Intelligence and the Military-Information-Security System of the Zionist Regime* Proceedings of the International Conference on Artificial Intelligence and Iranian World Studies,

Bazarkina, D. (2023). Current and Future Threats of the Malicious Use of Artificial Intelligence by Terrorists: Psychological Aspects. In *The Palgrave Handbook of Malicious Use of AI and Psychological Security* (pp. 251-272). Springer International Publishing. https://doi.org/10.1007/978-3-031-22552-9_15

Briefs, S. (2026). *Artificial Intelligence and the Future of Terrorism*.

Davis, A. L. (2021). Artificial Intelligence and the Fight against International Terrorism. *American Intelligence Journal*, *38*(2), 63-73.

Djoric, M., & Milosevic, T. (2021). Abuse of Artificial Intelligence for Extremist and Terrorist Purposes. *Serbian Political Thought*, 220.

Elyaari, H. R. (2024). *Geopolitical Explanation of Terrorist Groups' Activism in Balochistan Region after the Islamic Revolution of Iran*. Farhang-e Mehryad.

Ezeamalu, R. C. (2026). *Terrorism and Its Implication on Global Security in the 21st Century: The ISIS Experience in the Middle East 2020–2025* [Doctoral dissertation, Godfrey Okoye University, Enugu].

Fong, B. C. (2026). What Is Driving the US and China to Compete—and Potentially Fight—over Taiwan: A Neo-Offensive Realist Analysis. *China Perspectives*(145), 7-17. https://doi.org/10.4000/chinaperspectives.17896

Ford, N. K. (2026). *A Mixed Response to Terrorism in the Middle East*.

Ganaie, N. A. (2025). The Role of Artificial Intelligence in Radicalisation, Recruitment and Terrorist Propaganda: Deconstructing Violent Extremism and Reimagining Counterterrorism in Contemporary Digital Ecosystems. *Frontiers in Political Science*, *7*, 1718396. https://doi.org/10.3389/fpos.2025.1718396

Gholami, M. (2021). *Media Behavior of Terrorism: Prohibition of Media Services to Individuals and Terrorist Groups in International Law Documents*. Asar-e Fekr.

Hosseini, S. L., Arab-Tat, M., & Hosseinmardi, M. M. (2025). Smart Diplomacy and International Security in the Age of Digital Transformation: Analyzing the Role of Artificial Intelligence in Combating Cyberterrorism. *Diplomatic Interactions*, *3*(10), 301-339. https://doi.org/10.22034/dpiq.2026.555275.1057

Houser, T., & Dong, B. (2025). The Convergence of Artificial Intelligence and Terrorism: A Systematic Review of the Literature. *Studies in Conflict & Terrorism*, 1-24. https://doi.org/10.1080/1057610X.2025.2467891

Juelich, A. (2026). *'God Has Helped Us, and So Will AI': How the Terrorist Group Boko Haram Uses Frontier AI*.

Khoumich, A., Mliless, M., & Achamrah, M. (2026). The Role of Artificial Intelligence in Combating Terrorism: Exploring Capabilities and Challenges in the Dark and Deep Web. In *AI-Driven Policing and Urban Security in Smart Cities* (pp. 129-154). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-1234-5.ch007

Li, J., Dai, Y., Woldearegay, T., & Deb, S. (2026). Cognitive Warfare and the Logic of Power: Reinterpreting Offensive Realism in Russia's Strategic Information Operations. *Defence Studies*, *26*(1), 127-148. https://doi.org/10.1080/14702436.2025.2465678

Macdonald, S., Mattheis, A., & Wells, D. (2024). *Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online*.

Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. W. W. Norton & Company.

Mearsheimer, J. J. (2012). *The Israel Lobby and Offensive Realism*. Imam Sadegh University.

Muperi, J. T. (2026). Beyond Pure Power Politics: Cognitive and Cultural Dimensions of Russian Offensive Realism in Ukraine. *Problems of Post-Communism*, *73*(2), 124-137. https://doi.org/10.1080/10758216.2025.2467892

Olech, A. (2026). Terror-AI-sm: The Future of Artificial Intelligence in the Hands of Terrorists. In *Emerging Disruptive Technologies and Terrorism* (pp. 103-122). NATO Centre of Excellence Defence Against Terrorism.

Razmkhah, N. (2024). A Critique of the European Union's Draft Law on Harmonizing AI Regulations from the Perspective of Combating Cyberterrorism. *Tehran University Public Law*

Studies Quarterly, *54*(3), 1959-1985. https://doi.org/10.22059/jplsq.2022.343006.3086

Shiroudi, M. S., Hemmati, M., & Siahpoosh, E. (2020). Artificial Intelligence and the Future of Attacks by Takfiri Terrorist Groups. *Southwest Asian Studies Quarterly*, *3*(9).

Soliman, G. (2026). The Reshaped Terrorist Threat in the Middle East in 2025. *Counter Terrorist Trends and Analyses*, *18*(1), 92-98.

Turner, L. (2026). *Artificial Intelligence, Counter-Terrorism and the Rule of Law: At the Heart of National Security*.

Vashishtha, N. (2023). *Artificial Intelligence-Assisted Terrorism: A New Era of Conflict.*