Journal of Social Sciences Research & Policy (JSSRP)

GISSR Global Institute of Social Sciences Research

Warfare 6.0: AI Driven Threatcasting in Intelligence, COIN, and CT Strategies

Dr. Zeeshan Zaighum[1], Hasan Zuberi[2], Dr. Muhammad Jawed Aslam[3]

1. Assistant Professor, School of Media and Mass Communication, and Research Fellow at BCPR, Beacon House National University, Lahore.
2. Visiting Research Fellow at BCPR, Beacon House National University, Lahore.
3. Associate Professor, School of Media and Communication Studies, UMT.

Cite This Article: Zaighum, Z., Zuberi, H. & Aslam, M. J. (2026). Warfare 6.0: AI Driven Threatcasting in Intelligence, COIN, and CT Strategies. *Journal of Social Sciences Research & Policy. 4 (02), 138-144.*
DOI: https://doi.org/10.71327/jssrp.42.138.144

ISSN: 3006-6557 (Online)
ISSN: 3006-6549 (Print)

Vol. 4, **No.** 2 (2026)
Pages: 138-144

Key Words:
National Security, Threatcasting, Artificial General Intelligence, Counter Terrorism, COIN, Predictive Intelligence

Corresponding Author:
Dr. Zeeshan Zaighum
Email: jawed.aslam@umt.edu.pk

License:

Abstract: *Warfare 6.0 is the next generation of warfare. It will be defined by the shift from narrowed AI to Artificial General Intelligence (AGI). The integration of AGI with quantum computing, sentient programming, and advanced machine learning will transform threatcasting, a practice used in predictive intelligence and counter-insurgency. The study is based on existing literature and case studies. This study explores the broad-spectrum utility of AI driven threatcasting across kinetic and non-actions in intelligence, security, counter insurgency domains. The study poses that AI driven threatcasting will be useful in cyber, cognitive, intelligence, nuclear, counter-terrorism, and counter extremism domains. By ensuring real-time data analytics, actionable intelligence can be used to proactively mitigate any threat in the aforementioned domains. With tools like Neuro Cognitive Threat Analysis, quantum computing, and advanced machine learning (AML); threatcasting can be transformed into more applicable and actionable field.*

Introduction

Technology is considered as the fundamental driver of the character of warfare, with each generation of warfare defined on the basis technological advancements. The contemporary fifth-generation warfare is also marked by its technological orientation focusing cyber capabilities, information warfare, and hybrid tactics[1]. As we look into the future, warfare will continue to evolve, with Warfare 6.0 or the next generation of warfare will be the next phase of conflicts. The paradigm shift in the theatre of conflicts will be manifested in moving beyond military engagements towards multidimensional tech-driven security environment. With Artificial Intelligence at its core, next generation of warfare will also augment machine learning, quantum computing and sentient programming. Amidst the shift from kinetic and hybrid actions, Warfare 6.0 will focus on undermining and subverting adversaries through and in technology. New security environment will encompass digital, cognitive, information, and intelligence domains altogether creating a much interconnected and more complex environment.

[1] Zaighum, Zeeshan, and Farasat Rasool. 2023. "Fifth Generation Hybrid Warfare in Pakistan: Mapping Hybrid Threats, State Interpretations, and the way Forward." IPRI Journal IPRI Journal.

AI Driven Threatcasting

One of the most significant shifts will be in the domain of threatcasting- a process and ability of predicting future threats. With sentient AI, threatcasting will also witness a fundamental shift. Therefore, it is important to study how Artificial Intelligence will be used for Threatcasting in military and intelligence.

While the contemporary discourse on the emerging warfare primarily focuses on technological innovations and breakthroughs, scholars argue that the evolution of next generation warfare is not only towards technology but also structural, cognitive, and strategic. The transition from narrow AI to sentient AI poses a fundamental shift in the very existence of the issue itself. Unlike conventional threats manifested through terrorism and insurgency, Warfare 6.0 commences a new era of adversarial competition that is enabled by AI. From inferential analysis to operational execution, AI assists planners in all phases of threatcasting. This has led to the imagination of deterrence, escalation, the widespread distributed lethality.

Additionally, complex geopolitical rivalries between technologically advanced countries particularly US, China, and Russia offer a broader and clearer strategic context to elucidate warfare 6.0. China's doctrine of 'intelligentized warfare' dominates its strategy to counter western AI centric military approaches. However, besides contextualizing this to state actors only, the dual use dilemma of AI blurs the distinction between civil and military threat vectors. With this not only technology itself is become decentralized but the means of conflict are also becoming democratized.

Furthermore, AI driven algorithms have paced up conflicts dramatically. Decision making process that would take hours historically will have to be done in hours. Speed as a variable situates several operational and tactical challenges such as erred escalation and misattribution. For Pakistan, a major challenge is balancing the integration of AI driven predictive technologies with governance frameworks that ensure resilience, strategic clarity and operational effectiveness in the era of algorithmic confrontation.

This means that threatcasting in warfare 6.0 should not merely be seen as a predictive tool but as a transformative strategic capability. The wider geopolitical and structural considerations validate this theoretical notion to study AI driven threatcasting.

However, traditional threat analysis models depend heavily on retrospective data and analogic frameworks describing probabilities. The epistemic transformation generated by AI driven threatcasting is often overlooked in scholarship. In AI driven threatcasting massive heterogeneous datasets can not only be analyzed in real time but in the time when wearables are common data ranging from digital footprints, sentiment analysis, cross-platform metadata signatures, and physiological information can be used to digitally forecast future prediction in a non-linear adaptive way. This will allow intelligence community to capture threat vectors in pre-emergent stage as conditions under which threats may materialize would already been forecasted. In addition to this, these dynamic threatcasts adapt to real world developments including weather changes, political shifts, social unrests, and their respective trends on digital media platforms. This will not only help in producing effective actionable research but also eliminate the limitations of traditional predictive intelligence activities. Conventional methods depend on human judgement that can be negatively influenced by mirror imaging, conformation bias, and recency bias. Besides this, human analysis also faces challenges in timely identifying implicit data patterns. Many scholars argue that algorithms are also not free from biases based on race, ethnicities, and religion. 'Algorithmic Mirroring' (when system reinforces patterns emerging from flawed data sets) is one of the challenges posed by biased algorithms wh. Yet, better programming can help overcome

these biases. This can also be addressed through a hybrid model of Human-AI analytical oversight.

Predicting future threats has always remained a challenge for intelligence officials, policymakers and researchers. When it comes to cyber and physical domains, threatcasting is an analytical framework that is used to predict future threats. Institutions and organization under this framework may predict future threats and make contingency plans. This predictive methodology will be revolutionized with the integration of Artificial Intelligence (AI)[2]. Threatcasting driven by super AI will employ advanced algorithms, innovative machine learning, and huge data analytics to not only predict future threats but also simulate outcomes, and actionable intelligence insights to counter threats. The conventional methods of threatcasting involve human judgements and linear models. Whereas, super AI driven threatcasting will be based on vast yet real-time data sets. It will also be able to identify implicit data and threat patterns which are otherwise non-existent for human eye. Therefore, generative AI driven threatcasting will be more accurate and empirical[3].

AI-Driven Threatcasting in the Cyber Domain

Gartzke (2013) argues that AI based threatcasting has fundamentally changed the whole process of predictive intelligence[4]. In the cyber domain, threatcasting employs machine learning algorithms, and neural networks, and advanced analytics based on Open Source Intelligence (OSINT), Signal Intelligence (SIGINT), Social media Intelligence (SOCMINT), and more importantly Cyber Threat Intelligence (CTI). AI will integrate different threat vectors with zero-day vulnerabilities to accurately predict future threats, threat patterns, and threat actors.

Several organizations include NATO is also working on AI driven threatcasting in cyber warfare. The future threats in the cyber domain may include “quantum cyber-attacks”[5]. According to Jowarder & Jahan (2024), quantum cyber-attacks will be undermine existing “cryptographic protocols, threatening critical national infrastructures (CNIs)[6]. AI as threat actor will identify and exploit vulnerabilities in machine learning systems. Therefore, predicting such threats in advance and accurately will be fundamental for defense of CNIs.

With the prevalence of 6G, attack threshold of cyber terrorism will also increase exponentially. The integration of quantum computing networks, autonomous systems, and Internet of Bio-Nano Technologies (IoBNT) with 6G internet will form a novel, sentient and immensely potent threat. Only a multilayered AI powered ecosystem based threatcasting will ensure situational awareness. For instance, future AI systems without requiring any human intervention will be able to isolate compromised nodes, autonomously patch vulnerabilities.

Additionally, AI-driven threatcasting will fundamentally shift the states’ conceptualization of ‘cyber deterrence’. Traditional cyber deterrence theory refers to discouraging potential attackers from carrying out hostile action by disrupting the gain and costs equation. However, deterrence based on punishment and denial becomes obsolete in AI powered autonomous environments. Widespread distributed, autonomous, and anonymous attacks will not be easily identified and attributed. AI-driven threatcasting can help in identifying and attributing such attacks by correlating behavioral signatures, carrying out

[2] Johnson, Brian David, and Natalie Vanatta. 2019. What the heck is threatcasting? Tempe: Arizona State University.

[3] Schmidt, Eric, and Jared Cohen. 2015. "The New Digital Age: Reshaping the future of people, nations and business." Asia-Pacific Journal of Rural Development 119-122.

[4] Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." International Security 41-73.

[5] Hiltunen, Elina, and Aki-Mauri Huhtinen. 2024. "The Holistic Framework of Time for Warfare." Futures and Foresight (Wiley) 1-13.

[6] Jowarder, Rafiul Azim, and Sawgat Jahan. 2024. "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection." World Journal of Advanced Engineering Technology and Sciences 330-339.

stylometry analysis that too in a very small period of time.

In offensive cyber operations, technologically advanced states are already experimenting with predictive targeting models which are capable of identifying adversarial CNI, identifying vulnerabilities, and carrying out attacks. These AI powered cyber intrusions are so lethal that human hackers will not be able to thwart such attacks. If these capabilities are ever acquired by non-state actors, only AI driven threatcasting will be able to preempt such attacks. In addition to this, anonymous cyber weapons in form of adaptive malwares also underscore the need for AI-powered threatcasting. These malwares when functional will be able to prioritize targets, adaptive evasion from any defense system, and self-replicate. Only a similarly adaptive and potent AI system can intercept these weapons.

Therefore, cyber domain operations in warfare 6.0 will not only require superior algorithms but also strategic frameworks capable of preempting adversarial attacks and autonomously thwarting them.

AI Driven Threatcasting in Cognitive Domain

One of the most interesting yet challenging areas in predictive intelligence is the cognitive domain. Human brain is still one of the most complex areas of research in intelligence studies. AI driven threatcasting in the cognitive domain is based on advanced nueroinformatics and neurolinguistic programming (NLP) to predict cognitive and informational threats[7]. Existing fifth-generation warfare aims to target perception to sabotage decision-making apparatus, and undermine public-institutional relationships[8]. Governments and institutions are still struggling to accurately identify threat vectors and threat actors. The situation will be far more complex in future, when warfare 6.0 will be based on sentient or super AI. Threat actors will deploy highly-targeted disinformation campaigns, real-time behavioral manipulation to destroy neuroplasticity of huge population. The situation will become more challenging when technologies such as AR, VR, MR will be used vastly. Threats such as the integration of NBIC (Nanotechnology, Biotechnology, Information Technology, and Cognitive neuroscience) will help develop augmented human operators and hybrid systems. Additionally, “Military Brain Science (MBS)” will commence a ‘mind superiority race’ among countries[9]. Therefore, a proactive threatcasting approach in the cognitive domain will require a more robust and a broad-spectrum AI driven neuro-cyber defense mechanisms to identify and mitigate any threat. These models will be able to integrate huge SOCMINT and OSINT data sets with NLP and LLM models to identify cognitive vulnerabilities[10].

Conceivably, cognitive domain will be the decisive theatre of Warfare 6.0. Disinformation will be precision and lethal strikes based on advanced neocortical warfare operations. By identifying neural vulnerabilities, behavioral susceptibilities, and ideological irrationalities, customized attacks will be carried out on individual and collective sense making apparatus. AI-driven threatcasting can optimize neurolinguistic programming models, neocortical mapping, and sentiment metametrics to detect pre-radicalization cures and intercept adversarial influence operations.

Furthermore, the Weaponization of immersive environments such as AR, VR, and MR also complicate the situation. These platforms can be used to corrupt collective political memory, manipulate emotional states, and implant exaggerated grievances. This makes these tools potent weapons of mass manipulation and ideological conditioning. Future threatcasting models must integrate immersive

[7] Wan, Zishen, Che-Kai Liu, Hanchen Yang, Chaojian Li Ritik Raj, Haoran You, Yonggan Fu, Cheng Wan, et al. 2024. "Towards Efficient Neuro-Symbolic AI: From Workload Characterization to Hardware Architecture." Ieee Transactions on Circuits and Systems for Artificial Intelligence 1-14.

[8] Zaighum, Zeeshan, and Farasat Rasool. 2023. "Fifth Generation Hybrid Warfare in Pakistan: Mapping Hybrid Threats, State Interpretations, and the way Forward." IPRI Journal IPRI Journal.

[9] Claverie, Bernard, and François Du Cluzel. 2023. Cognitive Warfare”: The Advent of the Concept of “Cognitics” in the Field of Warfare. NATO.

[10] Cluzel, Francois du. 2023. Cognitive Warfare, a Battle for the Brain. NATO.

environment monitoring to detect synthetic cognitive stimuli capable of influence mass manipulation.
As discussed earlier, NBIC driven technologies particularly neuro enhancement interfaces and bio digital implants will be blur the distinction between organic cognition and artificial augmentation. China, US, and Russia have already invested in Military Brain Science (MBS). Projects have been initiated to increase soldiers' cognitive resilience, and decision making speed though neurophysical interventions. All this will force intelligence communities to adapt to new information environment by focusing on digital cognitive hygiene frameworks which will be based on neuro security indicators, cognitive overload, sentiment manipulation patterns, and algorithmic volatility. This was a holistic strategic framework can be developed that can also serve as early warning system when and if a group or entire population is being targeted by some hostile actor.

Threatcasting in Intelligence Domain

Threatcasting is a sub-domain of predictive intelligence. Several countries have established R&D agencies. For instance, the US has "Intelligence Advanced Research Projects Agency (IARPA)" and "Defense Advanced Research Projects Agency (DARPA)", UK has "Advanced Research and Invention Agency (URIA)", Russia has "Russian Foundation for Advanced Research Projects", China has "Commission for Science, Technology and Industry for National Defense (COSTIND)". Whereas, Pakistan has newly established "Pakistan Advanced Research Projects Agency (PARPA)". Besides their mandate, all the aforementioned agencies are vested in developing AI based predictive tools for threatcasting in future.

AI in intelligence will pose numerous national security and defense challenges (Sfetcu 2024)[11]. AI is all set to be integrated into intelligence tools that will help enhance predictive capabilities, increase operational-efficiency, and catalyze decision-making process (Vogel, et al. 2021)[12]. CIA has already developed a generative AI tool, Osiris that is synchronized with OSINT. Osiris is a chat bot that is effective for curating large pools of data into more sense-making information. It is based on Large Language Model (LLM) to condense OSINT (Ewbank 2024)[13]. Additionally, AI is also being used in SIGINT[14], and GEOINT[15].

Future trends of the integration of AI in predictive intelligence will be far beyond content curation. Super AI will help automate intelligence collection, integration, analysis and autonomous actions. The future threatcasting may include intelligence practices such as Neuro-Cognitive Threat Analysis (NCTA) that integrate Brain-Computer Interaction (BCI) and neuro-symbolic AI to decipher adversarial neuro-cognitive patterns and profiling[16]. Another threatcasting technique will be "Quantum Enhanced SIGINT" that will include real time decryption and hyperspectral interception using quantum computing[17].

Besides changing intelligence gathering techniques. AI-driven threatcasting will structurally change the way intelligence community is established. Siloed and stovepiped intelligence agencies working in

[11] Sfetcu, Nicolae. 2024. Artificial Intelligence in Intelligence Agencies, Defense and National Security. MultiMedia.
[12] Vogel, K. M., G. Reid, C. Kampe, and P. Jones. 2021. "The impact of AI on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability, and management." Intelligence and National Security 827-848.
[13] Ewbank, Jennifer. 2024. "The Role of Artificial Intelligence in the U.S. Intelligence Community: Current Uses and Future Developments." Aspeninstitue.org. October . https://www.aspeninstitute.org/wp-content/uploads/2024/10/Ewbank_Role-of-AI-in-USIC_Final.pdf.
[14] Weinbaum, Cortney, Steven Berner, and Bruce McClintock. 2017. "SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain." rand.org. December 5. https://www.rand.org/pubs/perspectives/PE273.html.
[15] Kumari, Nirmala, and CN Khairnar. 2024. "Al-Based Signal Intelligence for Real-Time Threat Detection." Asian Journal of Convergence in Technology 1-8.
[16] McCreight, Robert. 2024. "The war inside your mind: unprotected brain battlefields and neuro-vulnerability." Academia Biology 1-9.
[17] McKendrick, Kathleen. 2019. Artificial Intelligence Prediction and Counterterrorism. London: Chatham House .

isolation will be incompatible in interdisciplinary, interconnected ecosystem. It is also important to mention here that intelligence community must be federated for it will help curating vast pool of data. AI systems then can correlate multi agency data sets while maintaining operational efficacy.

Another important prospect of AI drive threatcasting is 'autonomous intelligence cycle'. Otherwise phased and compartmentalized intelligence cycle will be self-capable to collect data, synthesize findings, predict analysis and design course of action autonomously. Earlier discussed hybrid model will only require a human approval before initiating an action. CIA's project Osiris, and China's Skynet demonstrate similar approaches. AI powered threatcasting models present significant advantages in detection, precision, and situational awareness. In a time-savvy competitive theatre, these models can be decisive factor of victory over an adversary.

During grey zone conflicts, decrypting deceptive adversarial strategies is challenging. AI-driven predictive intelligence models can combine neuro symbolic approach and probabilistic reasoning to remove fog of war.

AI Driven Threatcasting and Counterinsurgency

Future operational theatres in counterinsurgency will require a fundamental transition from population-centric approach of intelligence gathering to AI powered predictive mapping. AI-driven threatcasting in counterinsurgency may include integration of multilayered intelligence gathering[18] (i.e. OSINT, HUMINT, SIGINT, GIS) through deep learning models. The models should be capable of identifying insurgent patterns, trigger events, and geographic volatility indices. Based on past and contemporary trends, the models will be able to perform predictive tasks including simulations, scenario building- enabling intelligence community and law enforcement agencies to ascertain probable insurgent actions, forecast escalation thresholds with far higher empirical veracity. With incoroboration of Artificial General Intelligence, this linear looking process will not become adaptive but also dynamic provided the system is linked with insurgent propaganda networks, local sentiment analysis, and ground level socio-political activities. The model will also be able to carry out red-teaming activities and with juxtaposing it with cognitive patterns, it can also suggest calibrated interventions with respective outcomes ranging from kinetic to non-kinetic actions. This AI enabled threatcasting model can be a perpetual learning framework for both strategic and tactical decision making in counter insurgency.

In addition, AI powered predictive analysis can carry out insurgent activity forecasting. By enabling localized conflict heat-mapping, and integrating demographic indices, future trigger events and insurgency activities can be predicted. Changes in cross border communication patterns, online propaganda discourse, and local communication cascades can be used to predict future events. Predictive model can identify kinetic and non-kinetic approaches in a preemptive manner. This will counterinsurgency planners to precisely execute actions minimizing collateral damage and ensuring long term stability.

Ethical and Legal Considerations

AI driven threatcasting in the context of warfare 6.0 offers transformative potential in both kinetic and non-kinetic operations. Yet, this intersection of AI and warfare also poses several ethical and legal challenges. Firstly, International Human Law is mandated to regulated armed conflicts. Lethal Autonomous Weapon Systems can cause increased collateral damage or even unintended civil causalities[19]. Such scenario may cause immense legal deadlock on accountability and attribution of

[18] Maguire, Paul. 2024. Security Management Magazine. October 1. https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2024/october/Integrating-Evolving-Technology-Intelligence/.

[19] Hua, Shin-Shin. 2022. "Machine learning weapons and International Humanitarian Law: rethinking meaningful human control ." George Town Journal of International Law 117-146.

action with commanders and operators. Secondly, AI driven threatcasting will also cause "Dual-Use Dilemma" meaning it can be used be both military and civil use[20]. Such immense power and capability can also reach non-state actors and terrorist groups that will further jeopardize national security. Thirdly, Artificial General Intelligence will still be based on machine learning algorithms which can have inherent biases. This can target or discriminate certain groups on populations[21]. Fourthly, AI driven threatcasting will be based on huge number of data raising immense and widespread privacy concerns.

Recommendations for Pakistan

1. Establish a joint civilian-military National AI Threatcasting Center, that must bring data scientists, quantum computing researchers, defense analysts, and cognitive neuroscientists at a single platform to develop and field real-time threatcasting. The threatcasting model should be tailor made for Pakistan's traditional and digital security environment.
2. Integrate Neuro-Cognitive Threat Analysis into intelligence doctrine. This can be done through training intelligence and operation officers on NCTA techniques. Relevant experts and strategists should be consulted for developing and testing training modules.
3. Collaborate with leading universities and academic institutions to establish domestic quantum computing testbed to promote research.

Conclusion

Warfare 6.0 offers a transformative convergence of AI and threatcasting in counterinsurgency and intelligence domains. AI driven threatcasting is the foundation of this warfare paradigm. It has the ability to revolutionize predictive intelligence across kinetic and non-kinetic operations. The spectrum of attacks in a broad spectrum of cyber-attacks, cognitive attacks, will pose novel challenges. By integrating quantum computing with advanced machine learning algorithms, future AI driven threatcasting will be more accurate and empirical. Nevertheless, AI driven threatcasting will also present several technical, legal, and ethical challenges. Newer technologies will require more adaptive legislations along with ample ethical considerations of warfare 6.0. The capability of predictive intelligence, tools like Neuro Cognitive Threat Analysis, and Quantum Computing will be fundamental in devising military and intelligence strengths.

[20] Ambrus, Éva. 2020. "Artificial Intelligence as a Dual-use Technology." Academic and Applied Research in Military and Public Management Science 19-28.

[21] Longpre, Shayne, Marcus Storm, and Rishi Shah. 2022. "Lethal autonomous weapons systems & artificial intelligence: Trends, challenges, and policies." MIT Science Policy Review 47-56.