



# INSIGHTS

Vol. 3, No. 1, January 2025

## *The Emerging Potential for Quantum Computing in Irregular Warfare*

Quantum computing represents a paradigm shift in computational technology, poised to revolutionize industries including national security and defense. While the abilities of quantum computing still remain largely theoretical, significant progress is being made. Notably, experiments from companies like Google and IBM have demonstrated early examples of [quantum supremacy](#), where quantum computers outperform classical systems on specific tasks. These breakthroughs suggest that quantum computing is not only on the horizon but is considered an [inevitable advancement](#) that stakeholders should prepare for now.

Unlike classical computers, which rely on binary bits (ones and zeros) to process information in a linear or symmetric process, quantum computers utilize quantum bits, or “qubits,” which can exist in multiple states simultaneously. This can be a very difficult concept to grasp, but this capability enables quantum computers to perform complex calculations at unprecedented speeds, addressing problems that are currently unsolvable with even the most powerful supercomputers. As irregular warfare and gray zone conflict become increasingly reliant on advanced technology, the application of quantum computing in these domains has the potential to introduce new threats while also offering the possibility of new strategic advantages. Quantum computing could fundamentally alter how conflicts are managed and resolved in the 21st century.

AUTHOR: HANK HANNA - *Head of Technology Services*  
*Irregular Warfare Center (Morgan 6 Contractor)*



IWC MISSION: The IWC serves as the central mechanism for developing the Department of Defense's (DOD) irregular warfare knowledge and advancing the Department's understanding of irregular warfare concepts and doctrine in collaboration with key allies and partners.

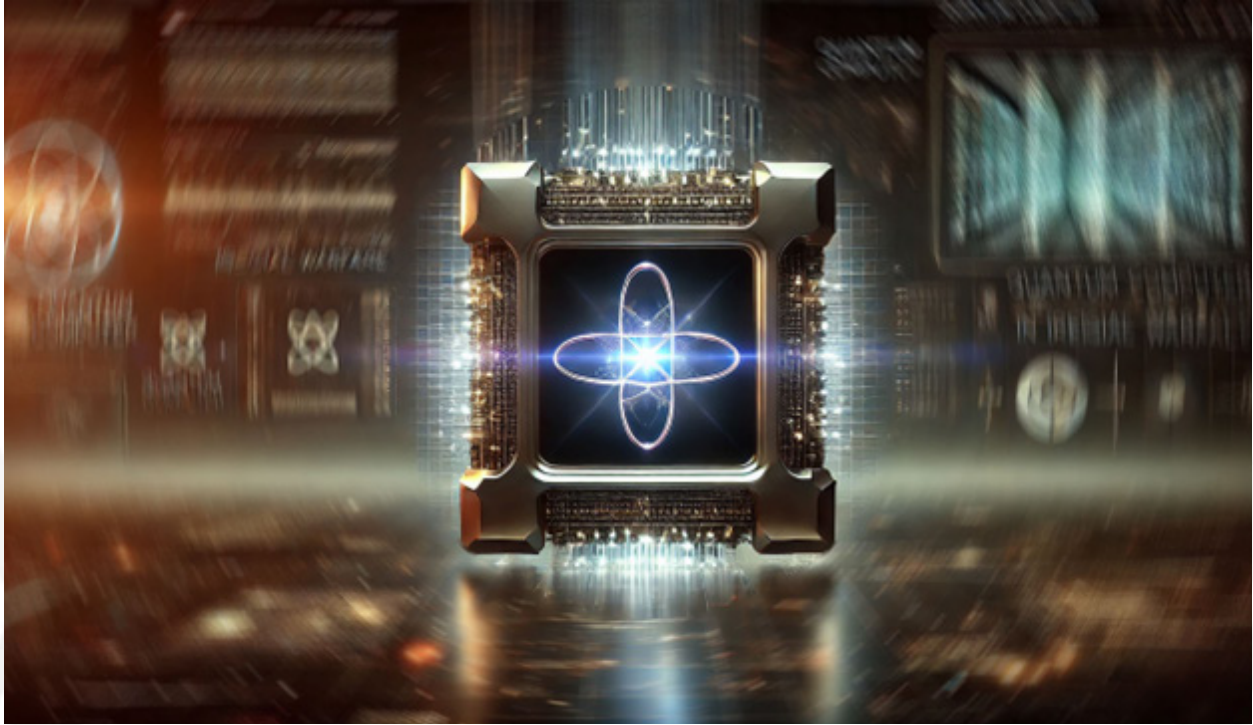


Figure 1 Image generated by AI using DALL.E and edited by H Hanna

## UNDERSTANDING QUANTUM COMPUTING

Classical computing, which forms the backbone of today’s digital infrastructure, operates on a binary system where “bits” of data are represented by either a zero or a one. These bits are processed sequentially, with classical computers executing tasks in a step-by-step manner. This approach, while powerful, faces significant limitations when confronted with complex problems that require immense computational resources. Quantum computing, however, [leverages the principles of quantum mechanics](#), allowing quantum bits, also known as “qubits,” to exist in multiple states simultaneously through a phenomenon known as superposition. In essence, while a classical bit must choose between 0 or 1, a qubit can represent both at the same time. This ability to perform parallel computations is further amplified by [entanglement, another quantum property](#), where qubits become interconnected in such a way that the state of one qubit directly influences the state of another, regardless of distance. To better understand the power of quantum computing, it can be helpful to visualize how it approaches problem-solving compared to classical computing. The podcast “[Ask A Spaceman](#)” used a very relatable analogy to illustrate this. Imagine you have a complex task that requires searching through a vast number of possibilities—like finding a small mouse hiding somewhere in an enormous mansion. What better way to find the mouse in the mansion than to use a cat, right? In this scenario, a classical computer would be like a single cat that methodically searches the mansion room by room. The cat can only be in one room at a time, and it must explore each room sequentially until it finds the mouse. If the mansion is vast, this process can be incredibly time-consuming. Now imagine a quantum computer as a cat with a unique ability: it can be in every room of the mansion simultaneously. A “q-cat” if you will. This q-cat doesn’t need to search room by room, but instead, can check every possible location in the mansion at once. The mouse’s location is found almost instantaneously, without the need to methodically explore each room. This analogy captures the essence of quantum

computing: the ability to perform multiple calculations simultaneously. By leveraging the principles of [superposition and entanglement](#), quantum computers achieve problem-solving speeds that are exponentially faster than those of classical computers.

## THE IMPLICATIONS OF QUANTUM COMPUTING IN IRREGULAR WARFARE

As quantum computing begins to emerge from theoretical research into practical application, it has the potential to significantly alter the landscape of irregular warfare and gray zone conflict, which thrive on complexity, ambiguity, and the exploitation of technological and informational asymmetries. For instance, a hostile nation equipped with quantum-enhanced decryption capabilities could intercept and decrypt military communications, rendering secure operations vulnerable and exposing critical intelligence. Similarly, quantum-enabled data processing could allow adversaries to analyze vast amounts of intercepted data in real-time, uncovering operational patterns or vulnerabilities. As it continues to evolve, the ability to rapidly process and analyze vast amounts of data could shift the balance of power, introducing entirely new approaches to conflict that were previously unimaginable. Quantum computing's promise lies not only in enhancing existing strategies but also in offering the potential to create new methods of engagement, forcing both state and non-state actors to reconsider their operational approaches. Understanding the possible applications of quantum computing in irregular warfare is essential for anticipating future threats and developing effective countermeasures, especially as adversaries seek to exploit these technologies for their own strategic gain.

## FEASIBLE APPLICATIONS OF QUANTUM COMPUTING IN IRREGULAR WARFARE

The following explores some of the most feasible applications of quantum computing in irregular warfare, highlighting how this emerging technology could enhance strategic capabilities and provide a competitive edge in an increasingly complex and unpredictable conflict environment.

### *Enhanced Cryptographic Capabilities*

One of the most widely anticipated applications of quantum computing is its ability to break traditional cryptographic systems. Classical encryption methods, which are foundational to secure communication and intelligence, rely on the computational difficulty of factoring large prime numbers—an approach that quantum algorithms like [Shor's](#) could easily dismantle. The implications are profound, as state and non-state actors could potentially intercept and decrypt sensitive communications, disrupting operations at multiple levels. This emerging threat has sparked a global race toward [post-quantum cryptography](#), which seeks to develop encryption methods resilient to quantum attacks. This arms race between offensive quantum decryption capabilities and defensive quantum-resistant encryption technologies is expected to be a defining aspect of future conflict landscapes. The [stakes for national security](#), espionage, and the protection of critical infrastructure are higher than ever as the U.S. and our adversaries develop increasingly sophisticated tools.

### *Optimization of Operations and Decision-Making*

Quantum computing's potential to optimize complex operations is particularly relevant to the logistical and decision-making demands of irregular warfare. With the ability to process vast datasets simultaneously, quantum algorithms can streamline logistics, resource allocation, and strategic planning. The advent of radar during World War II revolutionized military operations by providing near real-time intelligence about enemy aircraft movements, fundamentally altering how battles were fought and won. Similarly, quantum computing could revolutionize modern conflict by enabling

predictive conflict management, where geopolitical, economic, and social variables are analyzed concurrently to forecast potential conflict zones or flashpoints. A [study published in Stability: International Journal of Security and Development](#) demonstrates the feasibility and added value of machine learning in conflict prediction, primarily using classical computing methods. However, the principles explored in this research are directly applicable to quantum computing, offering a glimpse into how advanced quantum algorithms could enhance predictive conflict management. This capability would allow military and intelligence agencies to deploy resources and personnel preemptively, reducing response time and enabling a more proactive approach to conflict management. As these technologies evolve, quantum-enhanced decision-making processes could enable operators to navigate the unpredictable nature of these conflicts with greater confidence and precision.

### *Simulation and Modeling*

The ability to simulate and model complex battlefield environments is another critical area where quantum computing is poised to make a major impact. Traditional simulation methods frequently struggle to capture the inherent unpredictability of conflict that employs decentralized and fluid tactics. Quantum-enhanced wargaming could revolutionize this process by enabling military strategists to run numerous potential scenarios in parallel, exploring not only known strategies but also new and unforeseen outcomes. These simulations would offer unprecedented insights into adversary behaviors, operational risks, and tactical opportunities, leading to more effective strategic planning. Beyond battlefield tactics, quantum computing's capacity to model highly interconnected [cyber-physical systems](#)—such as power grids, transportation networks, and communication infrastructure—could help identify vulnerabilities and anticipate cascading failures caused by unconventional threats like cyberattacks or sabotage. This ability to test the resilience of critical infrastructure in real-time would provide decision-makers with actionable insights to mitigate risks and strengthen defensive measures, ensuring operational stability even under hybrid or gray zone pressures.

### *Influence Operations and Information Warfare*

Quantum computing's unparalleled data processing capabilities could significantly enhance influence operations and information warfare, which are central to modern irregular warfare and gray zone conflict. Quantum computing can analyze vast amounts of social media and information network data, identifying patterns, trends, and anomalies that may indicate adversary attempts to sway public opinion or spread disinformation. Beyond merely identifying these campaigns, quantum-augmented disinformation countermeasures could take things a step further. By simulating how disinformation spreads across networks, quantum computers could generate counter-narratives at scale and in real-time, disrupting adversary influence operations before they gain traction. This would mark a major advancement in defending against cognitive warfare tactics and information manipulation.

### *Countering Hybrid Threats*

Hybrid threats, which often blend conventional warfare with cyberattacks, misinformation, and irregular tactics, are particularly challenging to counter due to their multifaceted nature. Quantum computing could provide a powerful solution through quantum-enhanced [human terrain mapping](#)—a capability distinct from battlefield simulations. Unlike simulations that primarily focus on operational and tactical scenarios, human terrain mapping centers on the socio-political and economic environments in which conflicts unfold. This speculative but feasible application would enable the rapid analysis of vast datasets, such as population sentiment, resource distribution, and political instability, to identify patterns and trends indicative of social unrest, insurgent activity, or emerging conflicts across multiple regions.

For example, quantum-enhanced systems could integrate data from social media, economic reports, and historical conflict patterns to map areas of rising tension and predict where hybrid threats are most likely to materialize. By providing a nuanced understanding of the human environment, military and intelligence organizations could develop tailored strategies to mitigate risks before they escalate. This capability would complement battlefield simulations by addressing the broader contextual factors driving conflict, offering a more comprehensive approach to countering hybrid threats. As quantum computing continues to evolve, these advancements in human terrain mapping could transform how decision-makers navigate the complexities of gray zone conflict, where the line between peace and war is intentionally blurred.

## **APPLICATIONS THAT ARE OUTSIDE-OF-THE-BOX**

While many potential uses of quantum computing in irregular warfare are grounded in near-term feasibility, there are several speculative ideas that push the boundaries of current technology. These out-of-the-box concepts offer a glimpse into how quantum computing could revolutionize the future of conflict, introducing capabilities that are currently beyond reach but may soon become realities as the technology evolves.

### *Quantum-Enabled Autonomous Systems*

One of the most speculative but intriguing applications of quantum computing in irregular warfare is the development of quantum-powered artificial intelligence (AI) controlling autonomous systems. Unlike current AI models, which rely on classical computing limitations, quantum-enabled AI could rapidly process and adapt to vast amounts of battlefield data in real-time. This would enable autonomous drones or ground systems to operate with unprecedented agility, making decisions faster and more accurately in highly dynamic and unpredictable combat environments. These systems could evolve and learn in ways that current machine learning models cannot match, leading to a new generation of adaptive warfare technologies. Such quantum-powered autonomous systems could alter the balance of power in conflict zones, creating an edge where rapid adaptability is key. Additionally, these systems could operate in decentralized networks, coordinating seamlessly without the need for constant human intervention, further enhancing their effectiveness in conflict scenarios.

### *Quantum-Backed Surveillance Avoidance*

A more speculative, but equally transformative, application could involve quantum entanglement to develop untraceable communication networks. Quantum-backed surveillance avoidance would leverage the principles of quantum mechanics to create detection systems that evade traditional monitoring methods. Through the use of entangled particles, information could be transmitted in such a way that any attempt to intercept or observe the communication would alter its state, effectively rendering the transmission undetectable. This would provide a game-changing stealth capability, allowing operatives or military assets to communicate and maneuver without fear of detection. The potential impact on covert operations, intelligence gathering, and reconnaissance missions could be profound. If fully realized, this technology would make traditional surveillance obsolete, requiring adversaries to develop entirely new methods to counter these stealthy, quantum-enabled systems.

### *Strategic Deception at the Quantum Level*

Taking the concept of misinformation and deception to an entirely new level, quantum mechanics could be harnessed to create misinformation or decoy signals that appear legitimate until observed, a phenomenon deeply rooted in quantum mechanics itself. This could revolutionize deception operations.

By leveraging the peculiar nature of quantum superposition, a quantum-based deception operation could simultaneously present multiple layers of false information, making it nearly impossible for adversaries to distinguish between real and fabricated data. Strategic deception at the quantum level would offer a tactical advantage by forcing adversaries to waste resources and time on misleading targets. Furthermore, quantum-based deception could be used to manipulate decision-making processes, creating confusion or hesitation within enemy ranks. In an era where perception is often as important as reality, quantum mechanics could provide a powerful tool to shape the information environment in unpredictable and disorienting ways.

## QUANTUM LIMITATIONS AND CHALLENGES

While quantum computing holds immense promise, several significant technological challenges must be addressed before it can achieve its full potential, particularly in military applications. Chief among these is scalability. Current quantum computers remain in the experimental phase, with most systems only capable of processing a limited number of qubits. This limitation restricts their capacity to handle the large-scale computations necessary for complex defense scenarios. Moreover, quantum systems are highly sensitive to environmental factors such as temperature and electromagnetic interference, which can cause qubits to lose their quantum state in a process known as [decoherence](#). This instability severely impacts the reliability of quantum computers, posing a substantial hurdle to their widespread use.



Error correction is another critical challenge. Unlike classical computing, where error correction techniques are well-developed, quantum systems require much more sophisticated methods due to the inherent fragility of qubits. However, notable progress is being made in this area, with researchers developing [new quantum error correction techniques](#) aimed at mitigating these challenges. While these advancements show promise, creating quantum systems that are scalable, stable, and capable of real-time error correction remains essential to their future deployment in warfare environments.

Beyond the technical challenges, quantum computing in warfare raises important strategic concerns, particularly the potential for a quantum arms race. As nations strive to develop advanced quantum capabilities, there is a growing risk that the rapid pace of technological innovation could escalate into a race for quantum dominance. This competition may lead to destabilization, with countries prioritizing the development of offensive quantum technologies, such as encryption-breaking systems and autonomous warfare capabilities, while others rush to create defenses against these emerging threats. The ability to decrypt secure communications, manipulate information on an unprecedented scale, or deploy quantum-enabled autonomous systems has the potential to disrupt the balance of power, creating pressure for nations to outpace one another technologically. Additionally, the potential misuse of quantum technologies to fuel disinformation campaigns, conduct undetectable surveillance, or disrupt critical infrastructure further complicates the global security landscape. As quantum computing evolves, the establishment of international frameworks to regulate its use in conflict will be critical to mitigating the risks associated with unchecked quantum advancements.


## CONCLUSION

As quantum computing continues its transition from theoretical exploration to practical application, a comprehensive understanding of both its potential and its risks is essential for shaping the future of irregular warfare. The integration of quantum technologies into conflict scenarios will not only redefine strategic capabilities but also necessitate the creation of robust international norms, regulatory

frameworks, and multilateral agreements. These structures will be critical in ensuring that the rapid advancement of quantum computing does not trigger uncontrolled arms races, exacerbate global tensions, or undermine geopolitical stability. Although the full extent of quantum computing's impact on irregular warfare remains speculative, its disruptive potential is undeniable. As nations grapple with the opportunities and challenges posed by this revolutionary technology, quantum computing is poised to become a central element in the ongoing evolution of 21st-century conflict dynamics.



---



*The views expressed in these articles are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of Defense, or the U.S. Government.*