# Nuclear Deterrence in the Age of Emerging Technologies

**By**
**Muhammad Usama Khalid**

*Published: April 21, 2026*

The amalgamation of emerging technologies and nuclear weapons systems is significantly impacting the landscape of strategic stability. The primary problem associated with such technologies is their dual-use nature, such as Artificial Intelligence (AI), hyper sonics, quantum computing, and cyber warfare. These technologies are evolving more rapidly than the treaties meant to regulate them.

The most significant emerging technology is Artificial Intelligence (AI), a prominent dual-use disruptor. In the civilian domain, it can help process large amounts of data based on its training. Meanwhile, in the nuclear domain, it affects among other things, the nuclear decision making process.

The U.S. is currently considering incorporating AI into its NC3 modernization process while maintaining a human-in-the-loop policy for launches, using AI to monitor abnormal patterns in adversary movements. Russia, on the other hand, is developing AI-driven upgrades to its automated retaliatory strike system to ensure that if the country's leadership is decapitated, the system can autonomously verify a nuclear strike via seismic and radiation sensors before launching a retaliatory strike. These change decision timing and the deterrence dynamic.

The incorporation of hypersonic technology into delivery vehicles has revolutionized the exchange of weapons in warfare. The speed at which hypersonic systems travel can exceed Mach 5 (five times the speed of sound), potentially inducing miscalculation for an adversary, since it compresses the time window to clearly assess whether a missile is conventional or nuclear. In late 2024 and early 2025, India tested its Hypersonic Glide Vehicle (HGV) technology. Since these vehicles travel at such high speeds and at low altitudes with the ability to maneuver, it impacts the deterrence strategy between two nuclear countries. In response, Pakistan accelerated the Fatah series missiles, which are designed as flat-trajectory rockets. The geographical proximity of India and Pakistan compresses the decision-making window during a crisis.

The world's largest naval force, the U.S. navy, is currently integrating the Conventional Prompt Strike (CPS) hypersonic system onto Zumwalt-class destroyers. A Zumwalt-class ship may appear as a nuclear threat on radar but carries conventional weapons, risking warhead ambiguity for an adversary who might launch a nuclear strike if provoked. The recent exchange of delivery vehicles during the Iran and Israel conflict of 2024-2025 has shown the effect of hypersonic missiles in military operations. Iran used the Fattah-2 hypersonic missile, capable of Mach 5+ speeds with mid-flight maneuverability. Such weapon-delivery systems create strategic ambiguity for the adversary because they provide only a few seconds' window to decide whether to retaliate with conventional or nuclear missiles.

Advancements in quantum computing change warfare by providing more powerful algorithms producing vulnerabilities in secure systems. Nuclear launch codes, for example, are considered among the most secure encryption systems, which cannot be broken by classical computer methods. However, with advanced quantum computing methods, they become more vulnerable to hacking.

Additionally, Quantum sensing, which is facilitated with quantum electronic systems, allow for detection of minute changes in gravity or magnetic fields, which could produce systems that detect submarines, reducing their element of surprise. For example, China has made a huge leap by developing Quantum SQUID (Superconducting Quantum Interference Device) sensors. These devices may be able to detect the magnetic signature of US Ohio-class stealth submarines from miles away, threatening the ultimate nuclear deterrent.

Cyber warfare has recently moved to the forefront of modern warfare tactics with potential impacts on nuclear deterrence. Cyber warfare may produce uncertainties due to disruption of detection mechanisms and nuclear command and control that could produce unstable strategic situations. The classic Cold War model of Mutually Assured Destruction (MAD) was based on the visible, slow-moving, threat of nuclear weapons exchange. Cyber warfare introduces complexity and confusion. Thus, the deliberate nature of threats; instead, may instigate miscalculations driven by algorithms or false cyber signals.

A good example of how cyber operations can offset traditional military operations was the venture to physically damage Iranian nuclear centrifuges using malicious software (malware). The operation was carried out using Stuxnet malware installed from a USB drive that destroyed centrifuges without a single kinetic device. Similarly, Russian hackers have been carrying out cyber-attacks against Ukrainian energy infrastructure and government agencies since 2015. Vis-à-vis in 2025, during the ongoing Russia-Ukraine war, Ukrainian intelligence conducted a cyber-operation shutting down the Russian railway and affecting digital infrastructure.

A major problem lies with warhead ambiguity (conventional vs. nuclear), which poses a huge risk for accidental nuclear escalation. During the height of the May 2025 crisis between the two South Asian rivals, cyber operations were at their peak. Consequently, in the post-crisis scenario, India is enhancing its cyber deterrence. In future conflicts, any state's cyber space will be one of the primary targets; in a scenario where lines are already blurred, a single attempt to disrupt the cyber space of NC3 could be the initiating point of nuclear escalation.

The evolution of dual-use emerging technologies is fundamentally changing the traditional pillars of nuclear deterrence by compressing the action/reaction time required for rational decision-making. A major problem lies with warhead ambiguity (conventional vs. nuclear), which poses a huge risk for accidental nuclear escalation. In the volatile context of South Asia, dual-use technologies appear to destabilize a fragile strategic stability.

Ultimately, as machines outpace human thought in the decision loop, there is a danger that the resulting disruption is not just a technological arms race but the erosion of human-centric control, creating the risk of an accidental, algorithmically driven nuclear escalation as the defining strategic challenge of the future.

*Muhammad Usama Khalid is a Research Officer at the Balochistan Think Tank Network (BTTN), BUITEMS, Quetta. He can be reached at: usama.khalid.uk456@gmail.com. The views of the author are his own.*