MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Commentary

AI-Generated Zero-Day Vulnerabilities: Implications for Future Warfighting

Karanbir Singh Brar

June 08, 2026

Summary

Cyber security is no longer about protecting networks but about preserving combat power.

Introduction

Cybersecurity has long been viewed as a support function, largely focused on protecting military computer networks and information systems. This paradigm is now obsolete. As armed forces modernise through Artificial Intelligence (AI)-enabled platforms, autonomous systems, network-centric architectures, space assets, and digitally connected weapon systems, cybersecurity has evolved into a foundational layer of combat power. AI is now reshaping the character of warfare itself and is more consequential than ever in the machine-speed discovery and exploitation of software vulnerabilities.

Recent demonstrations by advanced AI systems such as Mythos AI[1]—which reportedly identified and chained vulnerabilities at speeds far beyond traditional human-led processes—provide a glimpse into a future where the timeline between vulnerability discovery and battlefield exploitation may be measured in hours/minutes rather than months. Even AI tools like ChatGPT-4 can exploit vulnerabilities and be exploited by non-state hackers.[2] This adds a concerning dimension to hybrid warfare, wherein targeting government, civilian infrastructure, economic and energy grids, state apparatus/govt functionalities, etc., can create disruption and portray the establishment negatively.

Discovering a serious zero-day threat once required elite researchers and months of effort. Advanced AI systems now scan codebases, identify weaknesses, build exploit chains, and launch attacks in hours—or minutes. In a Multi-Domain Operations (MDO) environment where land, air, maritime, cyber, space and electromagnetic effects are seamlessly integrated, this shift is a direct warfighting challenge. Future battles may be decided not by force size, but by which side sustains command and decision superiority under continuous automated cyber-attack.

The AI Zero-Day Revolution and the Algorithmic Battlefield

A zero-day vulnerability is an undisclosed flaw in software, hardware, or firmware that threat actors can exploit. It gets the name 'zero day' because developers and security vendors have had exactly zero days to identify, patch, or prepare a defence against the flaw before it can be actively weaponised. The traditional constraint on their discovery—human expertise and time—is disappearing. Modern AI tools map

[1] **"The 'AI Vulnerability Storm': Building a 'Mythos ready' Security Program"**, CSA-CISO Community, 1 May 1986.

[2] Margi Murphy, **"Google Says Hacker Used Mythos-Like AI for Software Tool Exploit"**, *Bloomberg*, 11 May 2026.

attack paths across millions of lines of code at machine speed, uncovering not isolated bugs but chains of weaknesses that combine into exploitable pathways.

Traditional battlefield outcomes were focused on force ratios, firepower, and mobility. As tech advances, emerging conflicts increasingly rely on data flows, network resilience, decision latency and machine-assisted command. The modern battlefield is now becoming an ecosystem of sensors, platforms, communications, AI models and decision-support systems. Zero-day vulnerabilities are hence becoming a potent threat, especially due to the collapse of the time between discovery and weaponisation.

Military organisations have historically relied on patching cycles designed for a world in which vulnerabilities remained unexploited for months. Adversaries with automated tools may now identify, exploit and deploy even during a conflict. They are not isolated technical issues or vulnerability management; these are operational vulnerabilities.

The Agentic Battlefield and Mindful Technology Infusion

Future operations will involve multiple interacting autonomous agents responsible for ISR, logistics, electronic warfare, targeting and decision support. In addition, a large share of military capability now resides in Operational Technology (OT): radars, missile systems, naval combat systems, satellites and battlefield sensors. All this increases the 'Attack Surface' for cyber exploitation.

The emergence of AI-generated zero-day vulnerabilities brings military modernisation full circle. Infusing technology into warfighting must be deliberate and mindful, because every digital capability introduced into the force also creates a potential attack surface. AI-enabled command systems, autonomous platforms, precision navigation, network-centric operations and intelligent logistics undoubtedly enhance combat effectiveness, but they also increase dependence on software, connectivity and data.

A zero-day vulnerability discovered and exploited at machine speed can transform a battlefield advantage into an operational liability. The critical question for military planners is therefore not merely what capability a technology delivers, but what vulnerability it introduces and what mission impact will result if that technology is compromised.

History suggests that resilient forces retain the ability to fight when technology is denied, degraded, or deceived. GPS-based navigation may be faster and more accurate. However, forces must still retain the ability to navigate through maps,

terrain association and celestial methods when satellites are jammed or attacked. AI-assisted targeting may compress sensor-to-shooter timelines, but commanders must still possess alternative procedures when algorithms fail or are manipulated.

A resilience assessment should therefore accompany every technology infusion: Can the mission continue if a zero-day vulnerability compromises the system? Is there a manual fallback, a parallel architecture, or an alternative means of execution? In an era when AI can discover and weaponise vulnerabilities faster than defenders can respond, the objective of modernisation is not simply to become more digital but to become more capable without becoming more fragile. The most effective military force will not be the one with the most technology, but the one that can continue to fight when that technology is under attack.

Cyber Exploitation as a Manoeuvre Capability

An increase in ‘attack surfaces’ for cyber exploitation in itself is not a serious vulnerability. However, an ‘AI-enabled automated cyber-attack’ can generate cascading effects across every warfighting domain. A single vulnerability in a satellite ground station can degrade space links, disrupt unmanned system feeds, slow ISR, extend strike timelines and reduce operational tempo—a flaw in cyberspace generating effects in space, air and land simultaneously.

An adversary need not compromise every system—only the weakest digital pathway that yields disproportionate operational effect. Automated tools greatly enhance the ability to identify such pathways across command systems, logistics networks, satellite assets, tactical communications, and defence-industrial supply chains. Future campaigns may feature continuous automated discovery of mission-critical vulnerabilities across military, civilian and industrial networks. Cyber exploitation in this context becomes operational manoeuvre.

Security by Design

With the above AI-enabled cyber threat challenges, security cannot be bolted on after development. It must be a core design requirement—alongside survivability, mobility, reliability and safety—with the explicit assumption that adversaries will apply advanced vulnerability discovery techniques throughout the system's entire service life. Every platform must be assessed not only for kinetic performance but for cyber resilience. The question is not whether vulnerabilities exist; it is whether the mission can survive despite them.

Testing platforms in isolation is insufficient; modern warfare requires testing systems-of-systems. National test beds must replicate operational networks, joint architectures, space assets, tactical communications, autonomous platforms, and defence industrial supply chains—and support continuous red-teaming with advanced attack tools. Military networks and architecture need to have the following:

- **Detection-First/Behaviour-Based Architecture**: Use endpoint solutions that stop active execution and exploit-chain behaviour the moment an attack occurs.[3]
- **Automated AI Red Teaming**: Leverage autonomous AI agents internally to find vulnerabilities in your dependency graphs before adversaries do, while maintaining human approval for all AI-generated fixes.[4]
- **Network Segmentation and Zero Trust**: Restrict lateral movement within your network to contain damage if a zero-day successfully executes.[5]

Critical questions must be answerable before conflict: Can missions continue under degraded communications? Where are single points of failure? How quickly can networks recover? Without realistic environments, many vulnerabilities remain invisible until conflict exposes them. This needs to be avoided at all costs.

Continuous validation in an MDO environment is necessary, as periodic evaluation is incompatible with the modern threat tempo. Every major exercise must incorporate realistic cyber-attack scenarios: communications disruption, data manipulation, autonomous system compromise and decision-support tool failure. Commanders must learn to operate in degraded digital environments as routine practice. The force that fights through disruption holds a decisive operational advantage. Resilience is now a warfighting capability.

Whole-of-Government Imperative

Automated vulnerabilities do not respect organisational boundaries. Military systems depend on civilian infrastructure; civilian infrastructure depends on private industry; private industry depends on global software supply chains. A whole-of-government approach is essential, integrating the armed forces,

[3] Akashdeep Bhardwaj and Authors, **"Proactive Threat Hunting to Detect Persistent Behaviour-based Advanced Adversaries"**, *Egyptian Informatics Journal*, Vol. 7, September 2024.

[4] Rob Smith, **"AI is Compressing Attack Timelines. Here's How Agencies Can Respond"**, NextGov, 27 May 1986.

[5] **"What is Zero Trust Architecture (ZTA)?"**, Paloalto Networks.

intelligence agencies, national cyber authorities, critical infrastructure operators, the defence industry, and academia around shared standards, information exchange, coordinated vulnerability management and joint exercises. An equivalent of Project Glasswing[6] of the US needs to be launched. National security is inseparable from national digital resilience.

India's simultaneous force modernisation, digital infrastructure expansion, indigenous defence technology development and AI investment create both significant opportunities and new attack surfaces. Priority areas include:

- Sovereign, indigenous security technologies for defence systems.
- Secure defence cloud and trusted semiconductor ecosystems.
- National cyber ranges and integrated test beds.
- Advanced defensive AI tools and vulnerability intelligence programs.
- Doctrine integrating cyber operations with MDO across digital, cognitive, electromagnetic, space and kinetic domains.

Future conflicts involving India will not be fought through kinetic means alone. Preparedness demands addressing these realities now.

Conclusion

AI-generated zero-day vulnerabilities mark a fundamental shift in the character of warfare. Cyber exploitation will increasingly function as a manoeuvre capability—degrading command, disrupting logistics, blinding sensors and slowing decision cycles. For military organisations, the implication is clear: cyber security must be embedded in force design, capability development, operational planning and doctrine. The future will belong to the force that maintains command integrity, preserves decision superiority and continues fighting under continuous digital disruption.

[6] **"Project Glasswing"**, Anthropic.

About the Author

Lt Gen Karanbir Singh Brar, PVSM, AVSM (Retd), is a former DG Armoured Corps and GOC Dakshin Bharat Area. Presently, he is a Distinguished Strategic Advisor with IIT Madras PRAVARTAK (Tech Innovation Hub of IITM).

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses