EXPLAINERS

What is Network-Centric Warfare?

Author: Ashutosh Kumar Singh • **Published:** September 19, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Network-Centric Warfare has shifted military advantage from individual platforms to the ability to connect sensors, commanders and weapons into a shared operational system. Its future will depend not only on faster information and AI-enabled decision-making, but on resilient networks that can withstand cyberattacks, electronic warfare and disruption. For India, this makes interoperability, jointness and resilient command-and-control increasingly central to modern warfare.

1. Introduction

The character of warfare has evolved with changes in technology, organisation and the way military forces perceive and exploit the battlespace. Industrial-era warfare emphasised mass firepower and physical concentration. The information age introduced a new source of advantage: the ability to collect, transmit and process information rapidly. Advances in sensors, digital communications, computing and precision systems gradually enabled geographically dispersed forces to operate as an integrated system. The basis of net-centric warfare is the

premise that the power of a force grows proportionate to the extent of networking that is prevalent among the weapons, sensors and the command-and-control element.

This transformation has become more significant as contemporary conflicts grow increasingly connected and technologically contested. Sensors, unmanned systems, satellites, command networks, electronic warfare and precision weapons now interact across considerable distances. Recent conflicts illustrate this shift through the extensive use of drones, digital networks, electronic warfare and rapidly evolving information systems. Network-centric warfare is the enabler that facilitates the shift from attrition style warfare to faster and more effective concepts of speed of command and precision/synchronisation.

However, connectivity also creates vulnerabilities. Network-dependent forces face risks from disruption, deception, cyber operations and electronic interference. Information overload further complicates decision-making. Several think tank reports identify network security, bandwidth, information overload and artificial intelligence as important challenges for the next generation of network-centric warfare.

NCW does not mean that platforms have become irrelevant. Aircraft, ships, tanks, missiles and soldiers remain the means through which military force is applied. What changes is the way these assets are connected and employed. The basic objective is to make a force see faster, understand better, decide earlier and act more effectively.

For India, NCW is particularly consequential as the country advances jointness and integrated military operations. It therefore involves not only technology, but also command structures, operational doctrine and institutional integration. The following discussion examines NCW's meaning, evolution, theoretical foundations, operational mechanism, contemporary challenges, recent applications and implications for India.

2. Definition and scope

Cebrowski states that "NCW is the military expression of the Information Age. It refers to the combination of strategies, emerging tactics, techniques and procedures, organisations and technologies that a networked force employs to create a decisive warfighting advantage." It provides a new conceptual framework to examine military missions, operations, and organizations in the information age.[1]

A US Congressional Research Service report defines NCO/ NCW as operations that rely "on computer equipment and networked communications technology to provide a shared awareness of the battlespace".[2]

D.S. Alberts, J.J. Garstka, and F.P. Stein define NCW as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[3]

Network-Centric Warfare can broadly be understood as an approach to military operations in which networked information and communications connect sensors, decision-makers and effectors to generate shared situational awareness and improved combat power.

The scope of Network-Centric Warfare extends beyond the mere integration of military communication systems. It encompasses the collection, transmission, fusion and exploitation of information across the battlespace. Thus, enhancing situational awareness, coordination and decision-making. Its application spans across land, maritime, air, space and cyberspace. It links diverse sensors, command structures and combat platforms within an increasingly interconnected operational environment. The concept therefore involves technological, doctrinal and organisational dimensions, including C4ISR, interoperability, secure communications and distributed C2. With the growing incorporation of unmanned systems, AI and MDO, the scope of network-centricity continues to evolve. It expands from connecting forces towards integrating information, decision-making and effects across domains.

3. Historical Evolution

The concept of NCW is rooted in the overall revolution in the nature of warfare created by the ICT revolution. The evolution in computer technology, satellite communication, networks, and precision-guided weaponry during the 1980s and early 1990s began to alter the way in which militaries gathered and used information. The Gulf War of 1991 served as a significant operational example of this trend. It proved that the combination of intelligence, communications, precision strikes, and C2 was superior to the individual use of each platform.

The concept was formally articulated in January 1998. When Vice Admiral Arthur K. Cebrowski and John J. Garstka published Network-Centric Warfare: Its Origin and Future in the U.S. Naval Institute Proceedings. They argued that the information age was producing a shift from platform-centric to network-centric warfare. Their formulation linked sensor networks, information systems and engagement capabilities to improved situational awareness, speed of command and self-synchronisation.[4]

NCW thus evolved beyond a purely technological concept to encompass the joint evolution of technology, doctrine and organisational structure. Subsequent US developments, including concepts such as ForceNet, were built on the same ideas.

NCW was therefore conceived as more than a technological upgrade. The advocates of NCW viewed it as a transformation requiring the co-evolution of technology, doctrine and organisational structures. Subsequent US initiatives, like ForceNet, transformed these ideas into operational practice. By the early 2000s, NCW evolved from an emerging theory into a broader framework for understanding information-enabled military operations. India was also discussing the concept at an early stage. In 2005, the Indian Army described NCW as an approach that could translate informational superiority into combat power by linking sensors, shooters and decision-makers.[5]

The current developmental phase is characterised by AI-driven decision-making, autonomous platforms, and predictive analytics. NCW has further evolved into mosaic and algorithmic warfare.[6] These developments represent shifting military operations from rigid, linear structures to adaptive, intelligent networks - kill chain to cross domain kill-webs.[7] It allows enhanced decision making and more precise target selection and engagement with minimum collateral damage and cost efficiency.[8]

Thus, NCW was never simply a story of acquiring computers and communication equipment. Its deeper evolution involved changes in technology, doctrine, organisation and command philosophy.

4. Theoretical Foundations

There is no single direct theory serving as a basis for NCW. It is rooted in several theoretical ideas that explain how information, connectivity and decision-making can generate military advantage. These ideas do not constitute a single theory of NCW. Instead, they provide the intellectual basis for understanding its logic.

Revolution in military affairs explains how major changes in technology, doctrine and organisation can transform warfare.[9] NCW emerged within this debate as information technology began to reshape military operations.

Systems theory specifically concepts from the general systems theory and complex systems and serves as a core theoretical foundation for NCW. It views military forces as interconnected elements rather than isolated platforms.[10] NCW applies this logic by linking sensors, command structures and weapons into an integrated system. The effectiveness of the whole can therefore exceed that of individual components operating separately.

John Boyd's OODA model focuses on decision speed at the centre of military effectiveness. NCW aims to strengthen each stage through faster sensing, information sharing and coordination. The aim is to compress the decision cycle and maintain an operational advantage.[11]

Network theory emphasises the value created through connections among nodes. Cebrowski and Garstka adapted this logic to warfare. They argued that linking geographically dispersed forces could improve information flows, coordination and combat effectiveness.

Information superiority is the central operational premise of NCW. It is not simply about possessing more data. It means developing a clearer and more timely understanding of the battlespace and converting that understanding into action.

Together, these foundations establish the core logic of NCW: connect the force, improve awareness, accelerate decisions and generate effects faster than the adversary. The theoretical foundation of NCW rests on a simple proposition: information becomes military power when it improves the quality and speed of decisions.

5. Mechanism: How Does Network-Centric Warfare Work?

Network-Centric Warfare works by turning connected information into operational effect. Cebrowski and Garstka's original model placed three elements at its centre: a sensor grid, an information grid and an engagement grid. The information grid acts as the connective layer. It allows information collected by dispersed sensors to reach commanders and combat systems with minimum delay.[12] [13]

In simple terms: Sensors detect ? Networks connect ? Information is fused ? Commanders understand ? Weapons act.

The process begins with sensing. Satellites, radars, aircraft, UAVs and other ISR assets collect information from the battlespace. Then, this raw data moves through communication networks for processing and fusion. The aim is not to generate more information. It is to produce information that is accurate, relevant and timely enough to support decisions.

The next stage is shared situational awareness. Information from different sources is combined to build a common understanding of the battlespace. Thus, reducing dependence on isolated platform-level information. It can also allow geographically dispersed units to coordinate their actions.

This awareness then supports command and decision-making. The decision is transmitted to the appropriate shooter or effector through the engagement grids. This generates new information, creating a continuous feedback cycle.[14]

The desired outcome is the speed of command and self-synchronisation. A well-informed force can act faster and coordinate more effectively without validation from top commanders for every action.

The easiest way to understand NCW is through the sensor-to-shooter chain.

The NCW Cycle: Sensors and ISR ? Communication Networks ? Data Fusion and Processing ? Shared Situational Awareness ? Command and Decision ? Shooter/Effectors ? Battle Damage Assessment ? Feedback into the Network

The ultimate objective is therefore not merely connectivity. It is shorter and more effective sensor-to-decision-to-shooter cycles.

6. Challenges and Limitations

Despite several advantages, NCW has few limitations and challenges. Its effectiveness depends on trusted and resilient network. A disruption to sensing, communication or command can weaken the entire chain. Its advantages therefore come with important vulnerabilities.

- **Cyber vulnerability**: NCW's dependence on digital networks makes it a prime target for cyberattacks, such as hacking, jamming or malware, which can disrupt communications or feed false data. A compromised node can affect the wider network and distort information reaching commanders. Cyber and electronic warfare have consequently become integral to the contest for network superiority.

- **Information Overload:** NCW can produce more information than commanders can effectively process. This can create analysis paralysis due to overload amid tensed situations in the battlefield. The challenge is therefore not only to collect data but also to filter and prioritise it. AI is increasingly being trained for this task.

- **Technological Dependence:** A networked force depends heavily on communications, satellites, data links and digital infrastructure. Disruption of such systems can reduce operational effectiveness. Therefore, network resilience is important as network connectivity.

- **Interoperability Issues:** NCW requires different services and platforms to communicate through compatible systems. Differences in equipment, standards and organisational procedures can create information gaps. This limits the effectiveness of networked operations.

- **Cost and Complexity:** Building a network-centric force requires high investment in communications, sensors, software and trained personnel. The challenge is not simply acquiring technology but integrating diverse systems into one reliable architecture. This remains a major hurdle for under-developed and developing nations.

7. Contemporary Phase and Future of NCW

NCW has now moved beyond its original focus on connecting platforms. Contemporary warfare shortens sensor-to-shooter cycles by increasingly combining networks, AI, space systems, UAVs, cyber capabilities and precision weapons. Recent conflicts have demonstrated this transition, while also exposing the vulnerability of networks to electronic warfare and disruption. The key change is that the network is becoming more than a communication pipe. It is becoming an intelligence and decision-making architecture.

The next developments are likely to dominate AI-assisted decision-making, autonomous systems, resilient communications and multi-domain C2. Current developments are focused on securing networks, managing growing data flows and using AI to reduce information overload. AI is an emerging element in planning and executing multi-domain operations. Although, present AI systems still have limitations. Advanced interfaces, such as augmented reality and brain-computer interfaces, will allow soldiers to interact seamlessly with networked systems. Thus, the future of NCW will depend less on simply creating larger networks and more on making them adaptive, secure, interoperable and resilient under sustained contestation.

8. Relevant Examples

8.1 Operation Desert Storm, 1991:

The Gulf War provided an early operational picture of network-centric warfare. Coalition forces connected airborne surveillance, satellites, intelligence systems, command centres and precision weapons. [15] AWACS played a crucial role by detecting and tracking Iraqi aircraft information. One documented example involved an AWACS crew detecting an Iraqi helicopter and directing an F-15E to the target. The aircraft then destroyed it with a precision-guided

bomb.[16]

The importance was not one weapon. It was the connection between them. Information moved from sensor to command system to shooter. This reduced the time between detection and engagement. Therefore, the Gulf War demonstrated the operational value of shared awareness and precision effects.

8.2 Operation Iraqi Freedom, 2003:

The 2003 Iraq War represented a clear application of network-centric principles. US forces connected sensors, command-and-control systems, communications networks and precision weapons widely across dispersed formations. Real-time information sharing improved situational battlefield awareness and enabling faster decisions by commanders.[17] Operation Iraqi Freedom provided an important practical demonstration of NCW by linking weapons, sensors and C2 systems.

The key advantage was speed. Forces did not always need to concentrate physically to concentrate firepower. Information allowed dispersed units to coordinate their actions. NCW therefore contributed to faster targeting and more synchronised operations.

8.3 Russia-Ukraine War, 2022- Present:

This war demonstrates how network-centric warfare has evolved beyond traditional military platforms. NCW in the Russia-Ukraine war revolves around shortening the "kill chain"- the duration to detect a target, share its coordinates, and strike it, using connected digital networks, drones and satellite internet. Ukraine’s Delta system combines information from drones, electronic intelligence, acoustic sensors, satellites and battlefield reporting into a shared operational picture. This allows commanders and units to identify targets and transmit information rapidly.[18] These networks can compress sensor-to-shooter cycles to minutes, and sometimes seconds. Ukraine had also relied on commercial satellite like Maxar Technology, Planet Labs, MDA and Palantir technology's Meta Constellation for data integration from large no. of commercial satellites for tracking Russian troops movement, equipment and logistics in real time while, SpaceX Starlink terminals for high-speed, jam-resistant communication, bypassing traditional fibre-optic or mobile networks targeted by Russian strikes.

Russia's approach to *setetsentricheskaia voina* (network-centric war) merges Soviet-era electronic warfare (EW), AI-assisted information operations and computer network operations to degrade adversary decision-making. [19]

The lesson is significant. A drone by itself is only a sensor. Its real value increases when its information reaches the right commander and weapon quickly. Therefore, the war illustrates the modern NCW model: connect multiple sensors, build shared awareness, shorten decisions and deliver effects rapidly.

9. Implications for India

For India, Network-Centric Warfare is no longer only a technological aspiration. It is becoming a national-security requirement. India faces two very different geographical theatres. It must also prepare for simultaneous pressure across land, sea, air, space and cyber domains. In such an environment, information must move faster than the threat. A force that sees first, understands first and coordinates first can gain a critical operational advantage. But speed alone is not enough. The information must also be trusted, shared and converted into action.

For India, Network-Centric Warfare is remains a security imperative. India faces threats across land, maritime, air, space and cyber domains. This makes shared situational awareness and rapid coordination increasingly important. The objective is therefore to reduce the gap between detection and action while keeping the force effective under disruption.

India has already built important elements of this architecture. AFNET and IACCS connect sensors, command centres and air-defence systems serving as digital backbone for the Indian Air Force. The Defence Communication Network provides secure connectivity across the services. More recently, Akashteer has strengthened the integration of Army Air-Defence systems with wider networks.[20] These capabilities gained particular relevance during Operation Sindoor, when IACCS, Akashteer and the Navy's Trigun worked together to provide a shared operational picture and support faster decisions.[21] India also launched Indian Radio Software Architecture (IRSA) Standard 1.0 in October 2025. It defines a common software framework for military radios through standardised interfaces, application programming interfaces, execution environments and mechanisms that allow communication waveforms to operate across different radio platforms. These efforts aim to improve secure and interoperable communications while reducing dependence on foreign communication technologies.[22]

Yet, India's challenge is larger than building more networks. Different systems must communicate seamlessly. Networks must survive cyber and electronic attacks. Data must reach commanders without creating information overload. This makes interoperability, resilience and indigenous communication technologies central to India's future NCW capability. India's development of Software-Defined Radios and the Indian Radio Software Architecture

reflects this direction.

The next step is the integration of NCW with multi-domain operations, space-based sensing, AI-assisted decision-making, autonomous systems software-defined communications and real-time data fusion. India's military leadership has already discussed moving from net-centric operations towards intelligent and all-domain warfare. India released a joint doctrine for multi-domain operations in August 2025, represents an important step.[23] After joint theatreisation, the Civil Military Fusion remains the next necessity enabling better NCW infrastructure.

The future objective is therefore clear: not merely a connected force, but a resilient force that can continue to sense, decide and act when the network itself is under attack.

Conclusion

Network-Centric Warfare has changed the meaning of military power. Its central idea is simple. A force gains advantage when its sensors, commanders and weapons can work as one connected system. But NCW is not about having more technology. It is about turning information into timely action. The real advantage comes from shortening the distance between seeing, understanding, deciding and acting. This was the central logic of the original Cebrowski–Garstka formulation.

Yet, NCW should not be treated as a formula for victory. More information does not automatically produce better decisions. A sophisticated network can still be deceived, disrupted or overloaded. An adversary can attack the network itself. Cyber operations, electronic warfare and attacks on critical digital infrastructure can therefore turn connectivity into a vulnerability.

This makes resilience as important as connectivity. The future force cannot depend on a perfect network. It must be able to fight through a damaged one. Redundancy, decentralised decision-making and human judgement will therefore remain important even as AI and autonomous systems become more capable.

For India, the issue is particularly significant. The country has moved from building individual communication systems towards a more integrated networked architecture.

Ultimately, the future of NCW will not be decided by who possesses the most advanced platform. It will depend on who can connect intelligence, preserve the network under attack, make sound decisions and deliver effects at the right moment. The decisive network, therefore, is not simply the fastest one. It is the one that continues to function when war becomes most

uncertain.

References:

1. R S Panwar. “Network Centric Warfare: Origins And Main Characteristics”.2017. Future Wars https://futurewars.rspanwar.net/category/concepts-and-doctrines/

2. Clay Wilson, *NCO: Background and Oversight Issues for Congress*, CRS Report for Congress, 12 Sept. 2026

3. D.S. Alberts, J.J. Garstka, and F.P. Stein. “Network Centric Warfare: Developing and Leveraging Information Superiority”. 2nd edition (revised), 1999.

4. Admiral Arthur K. Cebrowski, USN, and John H. Garstka “Network-Centric Warfare - Its Origin and Future”.1998. Volume 124/1/1,139. US Naval Institute https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future

5. Headquarters Army Training Command. “Indian Army Doctrine”. 2004. Indian Army https://www.files.ethz.ch/isn/157030/India%202004.pdf

6. A Vijay Kumar. ‘**AI and Autonomous Systems: Implications for India’s Defence Strategy**’. 2026.DRAS

7. Ashutosh kumar Singh. ‘What is Mosaic Warfare?’2026.Explainer. CNAWS

8. https://cnaws.in/explainers/what-is-mosaic-warfare

9. Ashutosh Kumar Singh. ‘What is Algorithmic Warfare?’. 2026.Explainer. CNAWS https://cnaws.in/explainers/what-is-algorithmic-warfare

10. Francis Domingo. ‘The RMA Theory and Small States’2014. Military and Strategic Affairs, Volume 6, No. 3, INSS https://www.inss.org.il/publication/the-rma-theory-and-small-states/

11. Bosio, Nick. “On War's Theory - Systems and Military Theory: Congruence Throughout History.” Thesis Proposal Review (PhD Milestone), 2016.

12. D. Anand, Ch. Raja and E.G. Rajan. ‘Network Centric warfare - Concepts and challenges’. 2018. Vol 3, No 14, International Journal of Networking and Communication Engineering https://www.researchgate.net/publication/327111113_Network_Centric_warfare_-_Concepts_and_challenges

13. Cebrowski A K, *The Implementation of Network Centric Warfare*, Office of Force Transformation, US DoD, 05 Jan 05, https://apps.dtic.mil/dtic/tr/fulltext/u2/a446831.pdf

14. Mark Sickert. ‘Network-Centric Warfare and the Operational Concepts of War: A Synergistic Effect’.2000. Researchgate

15. Admiral Arthur K. Cebrowski, USN, and John H. Garstka “Network-Centric Warfare - Its Origin and Future”.1998. Volume 124/1/1,139. US Naval Institute

16. Anuroop Iyenger. ‘Boosting Network Centric Warfare: View from the Base Level’.2023. Bharat Shakti https://bharatshakti.in/boosting-network-centric-warfare-view-from-the-base-level/

17. Conner Kerr. ‘How AWACS Changed Air Warfare: The Radar Plane That Gave One Side God’s-Eye View’. 2026. Afterburner Migflug https://migflug.com/afterburner/awacs-e3-sentry-changed-air-warfare-desert-storm-airborne-radar/

18. Mishra, Shitanshu. (2003). Network centric warfare in the context of ‘operation Iraqi freedom’. Strategic Analysis. 27. 546-562. 10.1080/09700160308450107.

19. Oscar Rosengren. ‘Network-centric Warfare in Ukraine: The Delta System’.2024. Grey Dynamics https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/

20. Nysret Buzhala. ‘Assessing Russian Network Warfare through the lens of the Ukraine Conflict’. 2026. Small Wars Journal. Reaearchgate https://www.researchgate.net/publication/404762833_Assessing_Russian_Network_Warfare_throu

21. Avalokit Singh Palhawat. ‘From Platforms to Networks: Assessing India’s progress in Network Centric Warfare’.2026. CNAWS

22. Ministry of Defence. ‘‘Operation Sindoor demonstrated Tri-Services synergy with unified real-time operational picture, enabling timely decisions, enhancing situational awareness & reducing the risk of fratricide; True example of Jointness: Raksha Mantri’’. 2025. PIB https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173013&reg=3&lang=2

23. Rahul Wankhede. ‘IRSA 1.0 and India’s Indigenous SDR Communications Architecture’.2026. MP-IDSA

24. Ashutosh kumar Singh. ‘What is Multi-Domain Warfare?’.2026. Explainer. CNAWS https://cnaws.in/explainers/what-is-multi-domain-warfare

The views expressed are those of the authors and do not represent the views of CNAWS.

Image Source: ChatGPT