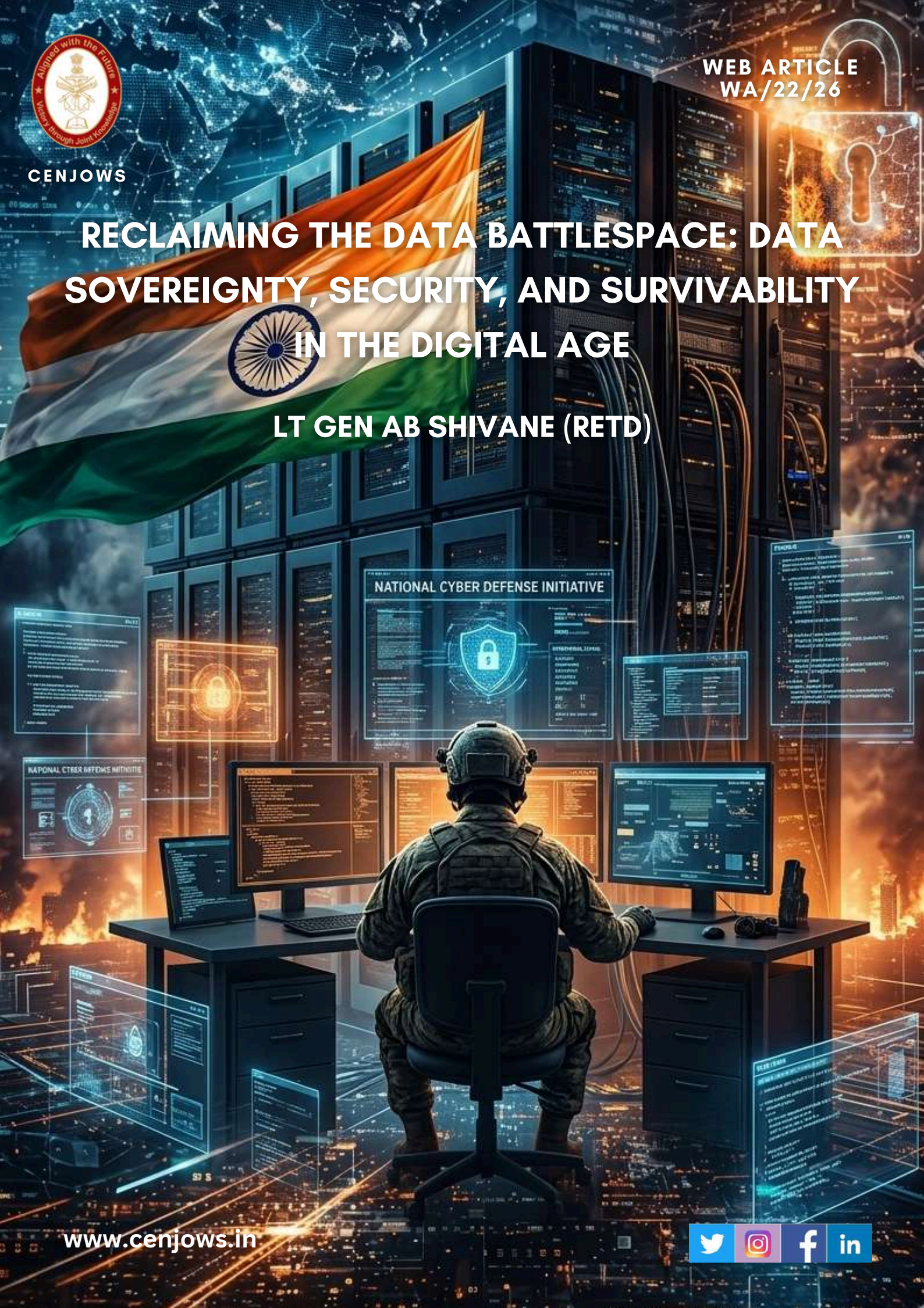
CENJOWS

WEB ARTICLE
WA/22/26

RECLAIMING THE DATA BATTLESPACE: DATA SOVEREIGNTY, SECURITY, AND SURVIVABILITY IN THE DIGITAL AGE

LT GEN AB SHIVANE (RETD)



CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Reclaiming the Data Battlespace: Data Sovereignty, Security, and Survivability in the Digital Age

Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd) is a former Strike Corps Commander and Director General of Mechanised Forces.

Abstract

Data control is no longer a peripheral technical issue. It now sits at the centre of how power is exercised. In India, this is already evident. Parts of the digital ecosystem remain tied to external systems, standards, and supply chains. In normal conditions, this works and delivers scale. However, in conflict or crises, it could expose vulnerabilities in access, integrity, and system control. The outcome is a subtle, persistent erosion of confidence in systems that have long supported decision-making across the military, political, and economic spheres.

This paper argues that data sovereignty, security, and survivability should be viewed not as separate entities but as a continuum. It further contends that localisation alone is insufficient for control. Data must be treated as a system from creation through movement, processing, storage, and eventual deletion. This requires industry collaboration, policy reforms, regulations, and trained human resources.

The paper concludes that data infrastructure will be a target in any future conflict. Disruption may occur through physical strikes, cyberattacks, or interference with supporting systems. Survivability and resilience, grounded in data hardening, a distributed architecture, and system redundancy, will be vital in such a contested environment.

Keywords: Data sovereignty; data security; survivability; digital infrastructure; data lifecycle; military planning; resilience; distributed architecture; cyber threats; strategic autonomy

Introduction

The future battlespace will depend on how effectively information moves across domains and reaches the decision point. At the core of present-day military capability lies the Command, Control, Communications, Computers, Cyber-Defence, Intelligence, Surveillance, and Reconnaissance (C5ISR) architecture, sustained by the flow, integrity, and timing of data. Control over this flow can no longer be treated as an enabling function in the background. It has direct operational consequences. When it is assured, it supports coherence and speed. When it is not, it introduces friction at critical points.

Data control, earlier viewed largely through a technical lens, has acquired strategic relevance. A significant proportion of sovereign data generated within India now moves through external digital ecosystems. In many cases, visibility over storage, processing, and access remains limited. Under normal conditions, this arrangement functions without evident disruption. Its limitations tend to surface only under stress.

The implications are gradual rather than immediate. Erosion, where it occurs, is not always visible in routine functioning. It becomes apparent when systems are required to perform under pressure. At that stage, questions of access, reliability, and priority begin to matter. Where these are uncertain, decision-making operates within constraints that are not always explicit but are nonetheless real.

In such a setting, sovereignty is affected in functional terms. Decisions may still be taken, but the conditions under which they are taken are narrower. This has consequences for both tempo and confidence. In the present environment, where data shapes targeting, algorithms extend reach, and AI reduces reaction time, these constraints carry operational significance.[i]

Data as a Determinant of Power

Conventional indicators of power, force levels, platforms, and firepower still matter. However, they no longer capture the full picture. Increasingly, advantage depends on the ability to access, process, and rely on data, particularly in contested conditions.

A point of concern in the Indian context is the extent of externalisation within critical data ecosystems.[ii] This has not been widely examined from a strategic perspective. In peacetime, such arrangements appear efficient and cost-effective. Systems remain functional, and dependencies are not immediately visible. The issue becomes clearer when conditions change.

In a more uncertain environment, dependence introduces variables that are difficult to control. Access may be subject to factors beyond the national authority's control. Prioritisation may not align with operational requirements. In a time-sensitive, decision-oriented operational environment, every delay or disruption incurs an operational penalty.

This is more than the use of technology or acquired capability. It's a matter of command over information flows that impacts military readiness, awareness, and decision dominance. Engagement with global digital networks offers benefits but also risks that are not evident in peacetime.

Operational Lessons from Contemporary Conflicts

Contemporary multidomain conflicts have highlighted the critical role of backbone data architecture in planning and execution within a network-enabled operational environment. In such a contested environment, data flow and network redundancy have played a critical role in operational outcomes. Thus, they can be both a critical strength and a vulnerability.

In the Russia–Ukraine war, targets have not been confined to traditional military targets. Data centres, power stations, and telecommunications infrastructure have been targeted to undermine command and control and degrade the kill chain. Thus, the tempo and precision in operations were largely affected by data degradation and disruptions.

In the recent Iran War 2026, a similar pattern emerged. Success has depended on the ability to integrate data from multiple sources for ISR and for precision missile or drone strikes. The criticality of data integrity and network redundancy has thus emerged as an important enabler. In the Strait of Hormuz, interference with navigation and tracking data has been used to disrupt shipping flow without direct engagement. This approach has added another dimension to warfare.

Overall, these conflicts highlight three key lessons: one, data is the new currency of war, and data centres will be priority targets; two, C5ISR and kill web architecture will depend on the networks and data that enable it; three, network disruption or spooking can be disastrous. Sovereign cloud architecture, reliable indigenous C5ISR, hardened and redundant communications, and data sovereignty, security, and survivability are no longer merely desirable; they are centres of gravity in a multidomain operation and battle-winning factors.[iii]

The issue is best understood in operational terms. The key to the success of multidomain operations lies in the convergence of interdomain synergy, enabled by interconnectivity across domains. Modern military systems depend on uninterrupted information flow. Even small interruptions carry consequences. Monitoring systems generate vast amounts of visual and other data. Logistics rely on real-time tracking and predictive modelling. Seamless data sharing among services is crucial for command networks. All these functions depend on data being available, accurate, and secure whenever needed. Weapons do not fail first. The data behind them does. The consequences are operational.

Structural Vulnerabilities in India's Digital Ecosystem

Indian digital infrastructure is a stratified reality. Indigenous capacity has become visible, but even some of the most vital layers still depend on systems, tools, and supply chains that are not necessarily within the country. The reliance is not recent, but in a hostile geopolitical context, it has greater consequences than ever before.[iv]

Other risks are less visible but no less serious. Small delays in data transmission can slow the tempo of operations. Jurisdictional questions can complicate access when it

is most needed. Even robust systems can collapse if multiple dependencies are attacked simultaneously.

The concern is not limited to deliberate intrusion. It relates to latency, access prioritisation, legal jurisdiction, and systemic fragility. Even small delays in processing or transmitting data, even in high-tempo situations, can alter the decision cycle. In the worst case, when it is most needed, access to vital datasets can be degraded or disrupted.

The difficulty lies in the fact that many of these weaknesses remain hidden until tested. Systems that appear stable may not have been exposed to the conditions they would face in conflict. Without such testing, confidence rests on assumption rather than on experience. This makes it harder to judge how the system will perform when it matters most.

Decision Superiority and the Data Lifecycle Approach

Data sovereignty, superiority, integrity, and security, along with resilience, are instruments of national power. When these pathways are extended or externally mediated, responsiveness suffers. The effect is rarely dramatic. It shows up instead as hesitation, reduced clarity, and fewer viable options at the moment decisions matter most.[v] Delayed control is, in practice, diminished control.

In this context, data sovereignty must move beyond localisation. Data parked within borders reduces risks, but it leaves unanswered questions about actual command: who governs its flow, processing, or end use. Without that control, physical location offers limited assurance.

A more effective approach is to manage data control across its full lifecycle. This requires command over data from creation through transit, computation, storage, and finally secure deletion. Each stage poses distinct vulnerabilities and challenges that require layered safeguards to ensure data survivability and redundancy.[vi]

Far beyond simple hardware facilities, data centres underpin the broader digital framework. When they fail, the fallout spreads fast, hitting critical services and command functions. Their value is tested under stress, and their ability to switch to

backup systems, recover quickly, and function under degraded conditions gives them operational, military-grade resilience.

Securing the Data Infrastructure

At the centre of this framework is data centre security. These are not routine back-end facilities. They are the nerve centre of the system. Disruption at this level rarely remains contained and can spread across the wider national security architecture. Thus, fortifying data infrastructure must account for protection, multi-layered survivability, and redundancy.

Data storage must be distributed across locations, with access controlled, monitored, and logged. Data discipline is based on checks and verifications, not trust, and every access point must be scrutinised. Digital locks with multikey access must ensure there is no single point of vulnerability.

Physical security is equally important. This requires hardened infrastructure, including protected or underground facilities designed to withstand disruption. Systems that are not regularly checked for access control and survivability tend to develop weaknesses over time. These weak points are often exploited when conditions worsen.

Future-Proofing: Encryption, Quantum Risks, and Resilience Through Design

Encryption standards require greater focus. The emerging technology of quantum computing will require a shift towards algorithms that can withstand future decryption and disruptions.[vii] Encryption that cannot withstand future decryption is already a vulnerability.

Resilience and backups for data storage banks, power, and cooling links must be built into the system. Centralisation improves efficiency but concentrates risk.

Geographic distribution is crucial. Although a centralised structure can be effective during peacetime, it is prone to failure during war. An alternative is more robust, distributed networks, which can reroute traffic and provide load balancing in real time.[viii]

Equally important is the shift towards edge computing. Processing data near its source reduces reliance on remote facilities and shortens response times. This can make the difference between acting and missing an opportunity in operational theatres.

Survivability in a Contested Battlespace

Survivability begins with the simple assumption that systems are exposed and will be targeted. The digital backbone is a critical target in modern conflict. By definition, data centres are valuable targets, whether through cyber intrusion to corrupt data, electronic warfare to blind or isolate systems, or direct physical attacks to render them ineffective. Therefore, the comfort of peacetime standards and commercial best practice cannot be relied on in planning. Planning must reflect the more brutal logic of war, in which discontinuity is planned, recurrent, and, in many ways, coordinated across multiple spheres.

Survivability should be an inherent part of such an environment, not a layer of protection. This demands structural decisions to minimise exposure and reduce procurement time. One such measure, not a matter of preference but of necessity, is to locate vital facilities underground in response to the reality of precision targeting. The dimension and dispersion make it difficult for an adversary to deliver a decisive blow in a single attack. Likewise, defence against electromagnetic interference is no longer a fringe issue. The systems should be protected against natural and artificial interference that can render equipment ineffective without necessarily destroying it.

Equally important is the issue of autonomy during periods of stress. Even highly advanced internal systems are vulnerable when data centres depend entirely on external grids, cooling systems, or network pathways. The key to resilience lies in indigenous capabilities and a fallback data architecture that continues to function even in the face of disruptions. Systemic failure must be prevented at all costs.[ix]

Doctrinal Integration and War-Gaming

The integration of data infrastructure into military planning remains inconsistent. It is still approached as a technical enabler rather than an operational dependency. Joint

exercises and war-gaming rarely account for data denial, degradation, manipulation, or recovery under pressure. The backbone that supports modern decision-making is seldom pushed to failure. Systems are therefore assumed to work, largely because they have not been forced to break.

In conflict, disruption is unlikely to be gradual. It is more likely to be abrupt and disorienting. Access to reliable data may degrade without warning. The immediate effect is not silence but veracity and timeliness of data. Command chains that depend on steady data flows begin to feel constrained under these conditions. The lesson is straightforward. Partial functionality can be as constraining as outright denial.

The effects are cumulative. Situational awareness is compromised, even when data persists in fragments. The problem shifts from availability to usability. Delays in processing, verification, and dissemination begin to hinder coordination. This impacts the synergistic cross-domain application and increases the likelihood of errors.

This risk of data disruption cannot be assumed away. It has to be built into planning. Data disruption, degradation, and manipulation need to be treated as standard conditions in training and exercises. Training that assumes uninterrupted networks prepares forces for a scenario unlikely to unfold.

For this reason, the inclusion of data infrastructure, including data centres and network architecture, in joint exercises is essential. Realism demands simulation of denial, degradation, and recovery cycles. Systems must be forced to adapt, and personnel must learn to operate when the network is unreliable, contested, or partially compromised.

Doctrine will only remain relevant if it reflects this reality. In modern conflict, operational effectiveness depends as much on the resilience of information systems as it does on physical capability.[x]

Policy, PPP Model, and Regulatory Frameworks

The policy framework in India has begun to acknowledge the problem, but implementation remains uneven. The policy of ‘Atmanirbharta’ in defence must

prioritise the data ecosystem as an integrated framework. Without closer alignment, capacity may increase, but control will remain limited.

A structured public–private partnership model will be necessary to build and sustain capability. Indian technology firms have the capacity to design, develop, and operate large-scale data infrastructure. What is required is policy clarity and continuity. Without this, industry participation will remain tentative. Long-term commitments, along with clearly defined standards, are needed to ensure that commercial incentives do not diverge from national security requirements.[xi]

The existing regulatory framework needs a de novo approach, as it does not reflect the strategic importance of data. This requires an apex-level framework as a strategic mission to secure, store, and process data with requisite oversight mechanisms. Software dependencies, infrastructure vulnerabilities, data flow resilience, and encryption strength must be addressed.

Human Capital and Strategic Depth

The limiting factor is not infrastructure. It lies equally in the availability of personnel who understand how systems behave under strain. Building and securing systems is one part of the task. Knowing how they respond to disruption is another. That gap remains.

Data control cannot be left as a purely technical function. It has a direct bearing on strategic autonomy and operational success. Data control has become a command function rather than a technical skill. It assumes even greater criticality in a multidomain operational environment where data controls converge. India's integrated theatre command structure and its backbone will remain the data control. It requires systems that can absorb disruption, adjust to changing conditions, and continue to support decisions in contested and adverse environments.

The training should be oriented towards equipping human resources who are well-informed about the digital world and able to think outside the box to detect threats and develop mitigation strategies for stressed systems. Technical skill alone is not enough in the data battlespace. It must be supported by an understanding of what failure truly

means to a commander. This requires a cadre trained not only to operate systems but also to function amid data friction.

Way Ahead

India does not need another statement of intent on data security. It needs a shift in how the problem is addressed. The question is no longer what needs to be done. It is whether it will be done in time. At present, much of the system works because conditions are favourable. The real test will come when they are not. That is when the gaps will show.

The way forward begins with accepting that data now sits within the battlespace. It is no longer something that can be assumed to function in the background. Systems will be contested, interrupted, and, at times, partially denied. Planning has to reflect this. The assumption of steady-state performance, which holds in peacetime, does not carry forward into conflict conditions.

Even limited dependence on external systems will shape outcomes when pressure mounts. These dependencies may not be visible during routine operations, but they tend to assert themselves precisely when reliability is most critical. This is where margins narrow.

Addressing this will require choices that may not seem efficient in the short term. Building redundancy, maintaining excess capacity, and investing in domestic capability carry costs. Yet, these are an insurance for a nation’s national security.

Summary of Recommendations

- **Treat data infrastructure as a national strategic mission.** A national implementation framework should be issued within defined timelines, with clearly designated lead agencies and apex-level oversight. Fragmented ownership has to be eliminated early, not corrected later. Without this rigour, even efficient systems fail.
- **Create indigenous capacity in critical data sectors**. It's not an option; it's control. Sub-sectors such as cloud computing, high-performance computing,

and secure communications are critical to our defence and security. Any over-reliance on third parties can confer influence that may not be obvious in times of peace but may be a vulnerability in times of conflict. To reduce the threat, there needs to be continual investment and short-term sacrifice for long-term independence.

- **Centralised architectures need to be progressively rebalanced and distributed.** Nodes used to be monolithic, but now they are the targets. Distributed nodes, with processing and data spread across them, are more robust. They are harder to attack, and a failure in one part doesn't mean the system fails. But distribution shouldn't be blind; coordination and recovery processes must be in place.
- **Edge computing capabilities require targeted investment.** Deployment should focus on operationally sensitive environments where latency and network disruption directly affect outcomes. Processing at or near the point of action must become a standard design feature, not a specialised add-on. This enables more data processing and computation closer to the incident and decision-making, rather than over long distances, with time-critical implications. In a contested environment where communications are likely to be disrupted, this can be a decisive factor. It also aligns with the shift towards a degraded environment rather than "always connected".
- **Redundancy must be embedded at the design stage.** Redundancy is required in power, cooling, pathways, and storage to withstand shocks. It does raise costs, but systems built for efficiency alone tend to break when conditions shift. The choice is not between cost and redundancy. It is between controlled investment now and uncontrolled failure later.
- **Doctrine and training must reflect contested conditions.** Systems are often tested in ideal conditions, which leads to an illusion of certainty. Training and wargames should include routine denial, disruption, and partial failure. The goal is not to demonstrate that systems are effective, but rather to test their adaptation and resilience in the face of disruption. Doctrine will only remain relevant if it reflects this reality.
- **Legal and regulatory mechanisms require an overhaul.** Existing frameworks rely too heavily on static certification in a domain that is constantly

evolving. A shift is needed towards persistent monitoring, periodic audits, and tighter control over access and usage. The issue is not technology alone. It is one of governance. Effective enforcement will depend on coordination across multiple agencies, where alignment is often uneven, and accountability is diffused.

- **Private sector participation should be institutionalised.** Innovation in data technologies is largely driven outside government systems and cannot be treated as peripheral. Engagement must be structured, with clear policy backing and defined roles. The objective is sustained partnership, not absorption. Long-term arrangements, supported by trust and clarity, will be essential to translate private capability into operational advantage.
- **Human capital development needs sustained focus.** A specialised cadre with cross-domain expertise should be built through structured career pathways rather than isolated training interventions. Operational familiarity with degraded environments must be treated as a baseline requirement.
- **Survivability must anchor system design**. Systems will be targeted. Some will fail. The aim is to ensure continuity and recovery despite disruptive attacks. This requires an integrated approach that combines prevention and recovery through protection and redundancy.

Conclusion

The competition is not just about who can develop superior capabilities; it is also about who can sustain and restore those capabilities under attack. The capacity to protect, maintain, and repair data systems under duress will influence operational decisions in ways that may not be immediately apparent but are important.

The challenge in India is not a lack of understanding. The problem is implementation. Much of what is in place today works only because it hasn't been under prolonged stress. That is a fragile comfort. Conflict will not be stable and permissive, and permissive systems don't necessarily adapt to conflict. So, the challenge is not to start afresh but to execute clearly and rigorously and to prepare for conditions that are more difficult than those faced to date.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

ENDNOTES

[i] U.S. Department of Defence, *DoD Data Strategy*, 2020. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-Data-Strategy.pdf

[ii] Lucas Kello, The Virtual Weapon and International Order (Yale University Press, 2017). https://yalebooks.yale.edu/book/9780300226295/the-virtual-weapon-and-international-order/

[iii] NATO CCDCOE, *Cyber Threat Landscape Reports*. https://ccdcoe.org/research/cyber-threat-landscape/

[iv] Joseph S. Nye Jr., *The Future of Power* (PublicAffairs, 2011). https://www.publicaffairsbooks.com/titles/joseph-s-nye-jr/the-future-of-power/9781586488919/

[v] RAND Corporation, *Multi-Domain Operations Research*. https://www.rand.org/topics/multi-domain-operations.html

[vi] Government of India, *National Cyber Security Policy*, 2013. https://www.meity.gov.in/writereaddata/files/National_Cyber_Security_Policy-2013.pdf

[vii] NIST, *Post-Quantum Cryptography Program*. https://www.nist.gov/pqcrypto

[viii] RAND Corporation, *Resilient Distributed Systems Studies*. https://www.rand.org/topics/cybersecurity.html

[ix] NATO CCDCOE, *Cyber Resilience and Infrastructure Protection*. https://ccdcoe.org/research/

[x] Challenges in handling of Data Security in Data analysis ", IJCSPUB - INTERNATIONAL JOURNAL OF CURRENT SCIENCE (www.IJCSPUB.org), ISSN:2250-1770, Vol. 14, Issue 4, page no.303-307, October 2024:https://rjpn.org/IJCSPUB/papers/IJCSP24D1033.pdf

[xi] Thales Data Threat Report - 2026 https://cpl.thalesgroup.com/ppc/data-threat-report?utm_source=google&utm_medium=cpc&utm_campaign=&utm_content=&utm_term=thales%20data%20threat%20report&utm_source=google&utm_medium=cpc&utm_campaign=&utm_content=&utm_term=thales%20data%20threat%20report&gad_source=1&gad_campaignid=22494063008&gbraid=0AAAAAD_tGUQpPeAO0hYBGYbT59KYNbC2V&gclid=EAIaIQobChMIr6uZiOGAlAMVxYVmAh0g-DsUEAAYASAAEgKk4PD_BwE