COMMENTARIES

Beyond the Kill Switch: Why Cyber Resilience Must Become a National Security Priority

Author: Abhay A. • **Published:** November 14, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

As India accelerates its digital transformation, cybersecurity must evolve beyond preventing attacks towards ensuring operational resilience. Recent global incidents involving government digital services and connected infrastructure demonstrate how cyber vulnerabilities can threaten service continuity and produce real-world economic consequences. This article examines the growing risks posed by AI-enabled cyber threats, legacy industrial systems and third-party dependencies. It argues that India must move beyond compliance-driven cybersecurity towards a comprehensive national cyber-resilience framework built around proactive threat detection, critical infrastructure protection, institutional preparedness and rapid recovery capabilities.

1. Introduction: Is Shutting Down Systems Really the Best We Can Do?

Whenever a major cybersecurity threat emerges, governments and institutions often find themselves resorting to a familiar emergency measure: taking systems offline, isolating networks, suspending digital services and restricting access until the threat is contained.

There is an uncomfortable irony here. After investing billions in cybersecurity infrastructure, advanced firewalls, artificial intelligence-driven threat detection and sophisticated security architectures, organisations can still find themselves with one of the most basic defensive options available: switching systems off.

Of course, shutting down an affected system is not necessarily a failure. In certain situations, it may be the most responsible course of action to prevent further damage. The real concern, however, is that even after substantial investments in cybersecurity, organisations may have few alternatives to suspending essential services when their defences are compromised.

In an economy where governments, businesses, financial institutions, healthcare systems and critical infrastructure increasingly depend on interconnected digital networks, the ability to prevent an attack is only one part of the security equation. The ability to withstand an attack, contain its impact and restore normal operations is equally important.

The uncomfortable truth is that absolute cybersecurity is an illusion. Every new technology introduces dependencies, every software component can create potential vulnerabilities, and every security improvement gives attackers another challenge to overcome. Cybersecurity is therefore not a destination where an organisation eventually achieves complete security. It is an ongoing process of anticipating threats, managing risks and adapting to an evolving threat environment.

The emphasis must consequently shift from security alone towards resilience: the ability to continue functioning, even when defences are tested.

2. From Data Exposure to Physical Disruption: Global Lessons

One of the biggest challenges in cybersecurity is the gap between recognising risk and actually preparing for it.

Across industries, particularly among small and medium-sized organisations, cybersecurity is still frequently approached as a compliance exercise rather than an operational priority. Security measures are implemented to satisfy regulatory requirements, complete audits or demonstrate adherence to prescribed guidelines. However, passing an audit does not automatically mean that an organisation is prepared to withstand a sophisticated cyberattack.

This is partly a question of resources, but it is also a question of mindset. Organisations often underestimate the value of the data they hold, the interconnectedness of their systems and the potential consequences of a disruption.

Personally identifiable information (PII), financial records, operational data and customer databases are not simply administrative assets. They are valuable targets, and their compromise can have consequences extending well beyond the organisation itself.

More importantly, cyber incidents are no longer confined to stolen passwords, leaked databases or inaccessible websites. Digital vulnerabilities can translate into disruptions affecting physical infrastructure, essential services and wider economic activity.

Two developments offer important lessons.

The PHP vulnerability episode: When governments have to take systems offline

In October 2026, critical vulnerabilities in PHP, a programming language widely used to operate websites and applications, prompted precautionary shutdowns of government digital services in the Netherlands. The episode illustrated how a vulnerability in a widely deployed technology can affect multiple organisations simultaneously.

Importantly, these shutdowns were precautionary measures rather than evidence of successful intrusions. Nevertheless, they exposed an important operational challenge: when a widely used technology develops a critical vulnerability, organisations may have to choose between maintaining digital availability and containing potential risks.

Europe's supermarket refrigeration incidents: When digital vulnerabilities become physical risks

Reported cyber incidents affecting supermarket refrigeration systems in Europe during October and November 2026 highlighted another dimension of cyber risk. Disruptions to temperature-control systems reportedly forced retailers to discard food and temporarily interrupt operations.

These incidents demonstrate how vulnerabilities in connected operational systems can translate into physical and economic consequences. Systems that may appear peripheral to an organisation's core IT infrastructure can, in reality, be essential to its daily functioning.

The implications extend beyond financial losses to food safety, supply-chain continuity and public confidence.

3. India's Digital Transformation and the Need for Greater Cyber Resilience

India has made remarkable progress in building digital infrastructure. Initiatives under Digital India and the expansion of Digital Public Infrastructure have transformed how citizens access financial services, government benefits, identity systems and essential public services. However, the expansion of digital infrastructure also increases the country's exposure to cyber risk. As government services, financial systems and critical infrastructure become increasingly interconnected, a vulnerability in one part of the ecosystem can have consequences extending well beyond the organisation in which it originates. India's challenge is therefore not simply to digitalise faster, but to ensure that security and resilience develop at the same pace.

Three areas deserve particular attention.

Artificial intelligence and the changing threat landscape

Artificial intelligence is changing the speed and economics of cyber operations. From allowing malicious actors to automate reconnaissance, produce convincing phishing messages, it is overall increasing the scale of certain cyber campaigns. While AI does not independently make every attack sophisticated, it lowers barriers to entry and increases the potential reach of malicious operations. India must therefore strengthen continuous monitoring, threat intelligence, vulnerability management and proactive threat detection. The emphasis should move beyond responding to incidents towards identifying weaknesses before they are exploited.

Critical infrastructure and operational continuity

India's dependence on Operational Technology (OT), Industrial Control Systems (ICS) and SCADA environments makes industrial cybersecurity a national security concern. Power generation, water treatment, manufacturing and transportation increasingly depend on connected technologies, many of which include legacy components not originally designed for contemporary cyber threats.

Third-party and supply-chain dependencies

India's digital ecosystem increasingly depends on cloud providers, software developers, managed service providers and technology vendors. This creates vulnerabilities beyond the direct control of individual organisations. A weakness in a

third-party service can potentially expose multiple interconnected entities. Cybersecurity must therefore extend beyond individual organisational boundaries. The security of vendors, contractors and technology partners should be considered an integral part of the wider digital ecosystem.

4. Conclusion: Towards a National Cyber-Resilience Framework

The idea of absolute digital security needs to be abandoned. In an interconnected digital economy, no organisation can realistically guarantee that it will never experience a cyber incident. But accepting that breaches are inevitable should never mean accepting that disruption is unavoidable.

For India, this requires a shift from a predominantly compliance-driven approach towards a broader national cyber-resilience framework.

Cybersecurity cannot remain an annual audit exercise or a collection of documents prepared to satisfy regulatory requirements. Organisations, particularly those operating critical services or handling sensitive information, need to invest in dedicated security capabilities, regular risk assessments, incident-response arrangements and tested recovery mechanisms.

Small and medium-sized enterprises also need greater access to affordable security services, technical guidance and capacity-building programmes. Cybersecurity should be understood as an investment in operational continuity rather than simply an additional compliance expense.

India must also strengthen the protection of legacy infrastructure and industrial networks, while extending security requirements to third-party service providers and technology partners. At the national level, stronger collaboration between government institutions, CERT-In, sectoral regulators, private enterprises and research institutions is essential for threat intelligence sharing, coordinated response and preparedness.

Most importantly, there is a need to develop a different mindset towards data and cybersecurity. Institutions and individuals must recognise that data is not merely information collected and stored. When aggregated and analysed, it can reveal intimate details about individuals, communities and society. Its value, and the potential consequences of its misuse, must be understood at every stage of its lifecycle.

The protection of citizen data and critical digital infrastructure is ultimately a matter of national security. Public trust in digital services depends not only on their accessibility and convenience, but also on the confidence that they will remain secure and available when it matters most.