



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

BEYOND THE FENCE: NATIONAL SECURITY, BORDER MANAGEMENT AND EMERGING THREATS

~ *Rudrakshi Gupta*

INTRODUCTION:

Traditionally, the word 'border' brings to mind a physical line separating one country from another. Border security, therefore, was largely understood in terms of fencing, patrolling and preventing unauthorised entry. This understanding is no longer sufficient. With rapid developments in technology and greater global connectivity, threats to national security have also changed. Cyberattacks can originate from outside the country without anyone physically crossing the border. Drones can be operated remotely, while illegal immigration, organised crime, trafficking and cross-border terrorism continue to create serious security concerns.

As a result, effective border management today requires much more than physical barriers. Technology, intelligence, law and coordination between different government agencies have become equally important. At the same time, stronger security measures cannot operate outside constitutional limits. The real challenge for India is therefore to develop a system that can respond effectively to new security threats without unnecessarily interfering with individual rights and freedoms.

MEANING AND IMPORTANCE OF BORDER MANAGEMENT:

Border management refers to the steps taken by the State to secure its international borders while permitting lawful movement of people, goods and trade. The Ministry of Home Affairs

(MHA) deals with border security through measures involving infrastructure, technology and coordination among concerned agencies.¹

India faces a particular challenge because its borders pass through very different geographical regions, including mountains, deserts, rivers and forests. A security arrangement that works effectively in one region may not necessarily be suitable in another. For this reason, different measures such as fencing, floodlighting, Border Outposts and technological surveillance are used according to local requirements.

Technology now plays an important role in border security. The Comprehensive Integrated Border Management System (CIBMS) brings together security personnel and technologies such as sensors, communication networks and intelligence systems. This helps security agencies monitor border areas, identify suspicious activities and respond more effectively. It helps not only in preventing illegal entry but also in controlling smuggling, trafficking, terrorism and other cross-border crimes.

LEGAL FRAMEWORK GOVERNING BORDERS SECURITY IN INDIA:

India does not have a single law covering all aspects of border security. Instead, different laws deal with different types of threats. The Unlawful Activities (Prevention) Act, 1967 deals with unlawful and terrorist activities that may threaten the security and integrity of India.² The Border Security Force Act, 1968 provides the legal basis for the Border Security Force and its role in protecting the country's borders.³

As security threats have become more technology-based, the Information Technology Act, 2000 is also relevant in dealing with offences involving computers and digital systems.⁴ Similarly, the Immigration and Foreigners Act, 2025 regulates matters relating to the entry and exit of people, visas, travel documents and registration of foreigners.⁵ Together, these laws show that border security is no longer limited to guarding physical boundaries. It also involves immigration, digital security and preventing unlawful cross-border activities.

¹Ministry of Home Affairs, Border Management-I Division, Government of India.

²Unlawful Activities (Prevention) Act, 1967, No. 37 of 1967, India Code.

³Border Security Force Act, 1968, No. 47 of 1968, India Code.

⁴Information Technology Act, 2000, No. 21 of 2000, India Code.

⁵Immigration and Foreigners Act, 2025, No. 13 of 2025, India Code.

EMERGING THREATS TO NATIONAL SECURITY:

Cyber threats have become a major concern for national security because attacks can now be carried out from anywhere without physically crossing a border. Government networks, communication systems and other important infrastructure can be targeted remotely, and it may also be difficult to identify the person or country responsible for such attacks.

Drones and other unmanned technologies have created similar challenges. Since they can be operated from a distance, they may be used for surveillance or illegal cross-border activities. Artificial Intelligence can make security threats faster and more difficult to control. Cross-border crimes such as terrorism, trafficking, smuggling and illegal financial activities are also challenging because the people and evidence involved may be located in different countries. This makes cooperation between Indian and foreign authorities necessary. Therefore, border security today goes beyond physical borders and also includes the protection of digital systems, communication networks and cyberspace.

CONSTITUTIONAL CONCERNS:

The State has a duty to protect national security, but it must do so within constitutional limits. Technologies such as surveillance, facial recognition and biometrics can improve border security, but they may also raise concerns about privacy and individual freedom.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised the right to privacy as a fundamental right protected under Article 21 of the Constitution.⁶ The Court connected privacy with a person's dignity, liberty and individual autonomy. It also made it clear that the State cannot interfere with a person's privacy without proper justification. Without a proper legal reason, privacy cannot be restricted. In few cases, surveillance of personal information may be needed for national security, but there must be limits on how far authorities can go. Proper safeguards are thus important to protect personal information from misuse and to keep the authorities accountable.

NEXT STEPS:

India's laws and security system need to keep up with new technologies and changing security threats.

⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, (last visited on 13th Sept, 2026)

Laws should be reviewed regularly to deal with challenges such as cyberattacks, misuse of drones and organised cross-border crime.

There should also be clear rules for collecting and using personal or biometric data. People should be aware of why their information is being collected, who are able to access it and how long it will be kept. Proper safeguards are necessary to prevent its misuse.

Better coordination between security forces, police, intelligence, cyber and immigration agencies is equally important. Since crimes such as terrorism, trafficking and cybercrime often involve more than one country, India also needs to work with other nations by sharing information and assisting in investigations when required.

CONCLUSION:

Today, borders are not limited to physical boundaries between countries. Security threats can also arise through cyberspace, illegal immigration, financial networks and the misuse of technology. Therefore, India needs to look beyond traditional methods like fencing and patrolling and adopt measures that can deal with these new challenges.

At the same time, national security must not come at the cost of individual rights and privacy. Security agencies need enough power to protect the country, but they must work within constitutional limits. The aim should be to maintain a balance between effective border security and the protection of individual rights.