

The next war won't stay at the border: Lessons for India from Taiwan

The next conflict could arrive through a drone, a missile, a cyberattack, a communications blackout, or a wave of misinformation



[Manoj K Panigrahi](#), Aug 19, 2026

The annual Han Kuang exercise of Taiwan has served as a crucial testing ground for the combat readiness of its armed forces since its inception in 1984. In 2026, Taiwan is conducting the 42nd edition of these war games — an exercise that reflects not only the preparedness of its military but also the resilience of its society in the face of a potential conflict.

Taiwan's military is primarily tasked with defending the island against a potential Chinese attack. The roots of the Taiwan-China conflict stretch back to the Chinese Civil War of the 1930s. In 1949, Nationalist forces under Chiang Kai-shek, facing defeat on the mainland at the hands of the Communists led by Mao Zedong, retreated to Taiwan with the hope of eventually returning to

the mainland. That prospect, however, gradually faded with the passage of time.

The last major ground confrontation between the two sides took place in 1949 around the Kinmen Islands, where the Nationalists emerged victorious, helping consolidate their control over Taiwan and other territories under their administration. Since then, both sides have maintained a state of military preparedness. The prolonged confrontation has also drawn major external powers into the region, most notably the United States, which continues to support the maintenance of the status quo across the Taiwan Strait.

Taiwan's approach to military preparedness is noteworthy because its annual exercises are not confined to the armed forces. The Han Kuang drills are conducted in phases across the island and traditionally include air-defence exercises involving warning sirens, 30-minute readiness periods, emergency text messages to mobile phones, and strict traffic and evacuation controls in designated areas. Failure to comply with certain emergency measures can attract significant penalties.

For the first time, Taiwan has introduced a "digital disruption" module into the exercise to simulate attacks on communications infrastructure for 30 minutes. The objective is not merely to test military systems but to examine how government agencies, the military and civilians can function when conventional communication networks are disrupted. The exercise is, in effect, testing whether society can continue to operate when the digital infrastructure it takes for granted suddenly disappears.

Taiwan is also testing dispersed command-and-control operations, allowing smaller military units to make decisions independently on the ground depending on the circumstances. Such decentralisation could prove critical in a conflict where conventional command structures and communication networks may be disrupted.

Perhaps the most important lesson from Taiwan is that national defence cannot remain the sole responsibility of the armed forces. Taiwan has

increasingly adopted a “whole-of-society” approach to preparedness, seeking to equip civilians with basic knowledge and skills that could become vital during a crisis. Alongside government agencies, civil-defence organisations such as the Kuma Academy have taken on the task of training civilians in emergency response. The training includes basic first aid, evacuation planning, emergency preparedness and the effective use of essential supplies. The objective is not to replace the government or emergency services, but to ensure that citizens can remain self-sufficient during the critical initial stages of a crisis. The academy has reportedly trained more than one lakh civilians in these areas.

This is where Taiwan’s experience becomes particularly relevant for India.

India’s approach to military preparedness has traditionally focused on the armed forces, government agencies, state-level responses and civil-defence mechanisms, particularly in border regions. This framework has served the country in previous crises. However, the character of modern warfare is changing rapidly.

The proliferation of drones, missiles and other long-range systems means that the battlefield is no longer necessarily confined to the border. Aerial threats can potentially penetrate deep into a country’s territory, bringing civilian populations into the direct consequences of conflict. This does not cast doubt on the capabilities of India’s armed forces, emergency-response teams or security agencies. Rather, it highlights the need to ensure that civilians are better prepared to support these institutions during a crisis.

During Operation Sindoor 1.0, most aerial objects were reportedly intercepted before reaching civilian areas, with one aerial target being shot down near the outskirts of Hisar, Haryana. The larger lesson, however, is not simply about interception. Civilians also need to know what to do when an emergency occurs: where to take shelter, how to provide basic first aid, how to communicate during disruptions and, equally importantly, how to avoid creating panic.

The second lesson concerns misinformation. Modern conflicts are fought not only on land, in the air and at sea, but also in the information space. During Operation Sindoor 1.0, competition for “breaking news” led some television channels to rely on alarming graphics, sound effects and speculative coverage. Such reporting can amplify anxiety at precisely the moment when the public requires calm and credible information.

This is where the government and media organisations have a shared responsibility.

A structured system of public communication could help. The government could issue regular, concise updates at predetermined intervals during a crisis, providing citizens with verified information and reducing the space for rumours and misinformation. Media organisations, meanwhile, must recognise that national security reporting during an active conflict carries responsibilities beyond the pursuit of ratings and breaking-news headlines. Where clear guidelines exist, persistent and deliberate violations could invite appropriate regulatory action. The objective should not be censorship, but responsible communication during an emergency.

The third and perhaps most important lesson is the need for a comprehensive National Security Report and Strategy. India would benefit from a publicly accessible strategic document that clearly outlines the country’s major security threats, assesses emerging risks and sets out broad policy priorities for addressing them. Such a document would provide citizens, institutions, policymakers and the private sector with a clearer

understanding of the national-security environment. More importantly, it could help create a culture of national-security awareness from the grassroots to the highest levels of government.

For India, the lesson is not that Taiwan’s model can — or should — be replicated wholesale. India’s geography, population, security environment and institutional structure are fundamentally different. But the underlying principle is universal: a resilient nation is one in which the military,

government and society are prepared to function together under pressure. The next conflict may not announce itself at the border. It could arrive through a drone, a missile, a cyberattack, a communications blackout, or a wave of misinformation.

(Dr Manoj Kumar Panigrahi is an Associate Professor at the Jindal School of International Affairs, O.P. Jindal Global University, India. He is currently a 2026 MOFA Taiwan Fellow at National Chengchi University, Taiwan. Views expressed in the above piece are personal and solely those of the author. They do not necessarily reflect Firstpost's views.)