Social Media and Counter-Terror Operations

December 01, 2023

A counter-terror operation lasting for more than 24 hours in Rajouri's Kalakote in Jammu and Kashmir on 22–23 November saw five soldiers including two young Indian army officers and Lashkar-e-Taiba's (LeT) highly-trained 'commander' and his associate killed. Although the intent here is not to carry out a military analysis of the incident, it would be pertinent to mention that officers' casualty once again reinforces the fact that the Indian army leaders continue to lead the troops by example. The military lessons from this operation will certainly be drawn by the Army to modify its tactics and planning, as applicable. The opinion endeavours to flag the sensitive issue of usage of social media (SM) platforms, especially WhatsApp, during the course of such counter-terror operations.

Adverse Fallouts

Social media, as we all know, is very thoroughly abused by the terror outfits towards spread of dis-information as well as for recruitment purposes, among other objectives. The usage of social media platforms by the common people during the course of counter-terror operations, though, does not always portend well. In crisis situations such as natural disasters, messages on social media by the affected sections of people as also by relief providers do prove to be a force multiplier.

In most cases, SM platforms have been the only way of responding to natural disasters for disseminating real-time information, warnings, coordinating aid and relief and asking for funds, etc. However, given past experience, irresponsible spread of half-baked information on SM platforms could be counter-productive in several ways, especially when a counter-terror operation is in progress.

Vis-à-vis the recent Kalakote incident, a case in point were messages floating around on WhatsApp that gave finer and specific details concerning the ongoing gun fight between the troops and terrorists. These details, without any veracity, included name of the units involved in operations, location of operations, casualty to own troops to include their identity, etc. Shockingly, these details were in real- time, unofficial and against the norms of stealth and secrecy concerning tactical military operations. The origin of this particular message, amongst others, remained hazy and preceded any kinds of statement from an official source.

Such messages during an ongoing encounter with terrorists inevitably lead to adverse fallouts. It compromises the operational security by revealing tactics by giving out specific details of mobilisation of units, locations, and the quantum of troops involved. In the said context, the handlers of proxies are able to connect dots and deduce the operational plan of own forces. Such real-time information to the terrorists enables them to adapt their strategies.

Although not evident in the recent and similar terror incidents, SM updates could create panic among the public and hinder the authorities' ability to manage the situation effectively, through exaggerated account of losses by a terror strike that may inflame passions. It may also impact the morale of security forces and provide fuel to our adversary to carry out propaganda.

The reaction of common people, who are oblivious to the facts and cannot possibly appreciate the peculiarity of an unfolding operational situation, could get out of hand in extreme contingencies. This may manifest in display of anger through various means by the locals, instigated by sympathisers of terrorists.

Last but not the least, this variety of irresponsible message proliferation, adversely affects the families of soldiers that are involved in the operations. As per the norm, the next of kin of a soldier who is killed in action is informed about the loss through proper channel and according to a laid-down military protocol. A passage of information to the concerned family is processed after due verification for sake of authenticity. Information about demise through social media, prior to the same being conveyed officially by the army authorities, is the last thing that any suffering family would prefer. This is about dignity and military ethos.

Precedence and Counter Measures

Overall, the risks of compromising security and jeopardising the operations that irresponsible messaging could lead to, during such events, is highly problematic. We had seen this trend at its zenith during 26/11 Mumbai attacks, when the holed in terrorists continuously modified their actions, partially on their own initiative and partially due to the directions of their handlers from across the border, after getting status updates from the real-time media

coverage. The major difference in context between 26/11 and the present time period is the proliferation of messages on social media platforms like WhatsApp and X (formerly twitter), which is more challenging to control.

Given the popularity of SM, the army too has not been left untouched by its widespread usage and messaging on SM platforms is rampantly resorted to by its personnel, towards routine functioning. Being a mirror image of the civil society, one cannot blame the army for this. As mentioned, at times, reliance on SM becomes inescapable for everyday functioning of military units in terms of sharing updates and progress of routine activities.

In view of the above, it is needed that information leaks through social media be taken as the new normal by military planners and adequate measures are taken to mitigate the adverse fallouts, by factoring in such messaging. In addition to sensitising its personnel to obviate pilferage of information, proactive steps require to be planned so as not to let an information void shape up, for the same to be filled up by dis-information. Perhaps there is a requirement to decentralise the information management structure to make the same more responsive to dilute the ill-effects of half-baked messages that swarm the social media platforms during critical times when lives are at stake.

Views expressed are of the author and do not necessarily reflect the views of the Manohar Parrrikar IDSA or of the Government of India.

Keywords:

Social Media
Counter-Terrorism