

# Social Media - A Tool for the Military

---

UMONG SETHI

The year 2010 started relatively peacefully in the Kashmir valley. By the time summers arrived frenzy had been whipped up by issuing a calendar of seemingly peaceful protests. It set into motion a vicious cycle of *bundhs* in which invariably violence erupted resulting in police action leading to deaths of protesters followed by more *bundhs* and more violence that engulfed a large chunk of urban population of the Valley. It is now known that the entire orchestration of the protests was done by using social media on the internet and through SMSs on the mobile phones. The inimical elements not only coordinated violent protests but also stage-managed the places and timings on a virtually daily basis. The Arab Spring revolutions of 2011 in North Africa and West Asia were organised and sustained through social media platforms. The experiment was very successfully repeated by the group that organised protests in support of 'Jan Lok Pal' in 2012 in India. In January 2013, there was a surge of collective indignation as an aftermath of the gang rape of a 23-year old girl in Delhi. Cyber space was effectively exploited to connect and create massive public opinion resulting in some concrete action to revisit laws relating to 'Crimes against Women'.

We live in a cyber-era surrounded by smart phones, iPads and social media networks, YouTube, blogs and the like under the overarching shadow of internet. Life has changed as never before-it has turned digital. Shopping, reading, browsing news items, listening to music, paying bills, accessing bank accounts, looking for jobs, interacting with friends—all is now online. Logging into a desktop, laptop, iPad or a hand-held device opens avenues not only to a system

**The resulting changes in modern irregular warfare are both resulting from and embedded into socio-technological changes and have only been made by some militaries.**

but to a community. The new media has become social.<sup>1</sup> Facebook has 845 million active users and an average Facebook user has 130 friends. The average Facebook visit lasts 23 minutes. Twitter has 127 million active users and 54% of Twitter users use the service on their mobile device. LinkedIn now boasts of 200 million registered users. Skype has become a cheap and easy form of communication across the globe. Social media has assumed a vital role in social interaction not only for the youth but also for people of higher age groups who exploit it for professional and business use. Billions share experiences and

interact through the medium instantly. Snail mail, print or even the electronic media seem to have lost to this powerful medium in terms of speed and reach.

The new media that is a combination of the internet and software like Google, social networks etc. has three striking features: it diffuses mass media and social interaction; merges and blurs the message and its creator and costs of communicating being low has led to massive increase in number of participants. It has affected not only peaceful human interaction, but affected extremism, irregular war and terrorism in such an inexplicable way that is just about being understood by the militaries of the world. The resulting changes in modern irregular warfare are both resulting from and embedded into socio-technological changes and have only been made by some militaries.

The terrorists exploit the social networking tools and all the other internet technologies for internal communication among themselves and with their over ground workers. Funds, arms and even drug flows are tracked using the internet. Al Qaida used the internet to communicate with its cadres and sympathisers by disguising messages in their interactions over the net. They garnered support, spread the message of jihad and conveyed threats as well as messages to world powers using the power afforded by the new media. Propagators of the Al Qaida's ideology being 'media savvy' have sustained its influence using tools made available by the new media and have consequently ensured its survival despite suffering significant leadership losses.

In the highly networked environment of today where information flow is instantaneous, the local is increasingly getting linked to the strategic. A US drone attack targeting a hide-out located in a remote area of Afghanistan that results in casualties to women and children creates a furore over the new media despite

no media persons being available to report. It then implores within a short time, a response from the Secretary of Defense if not the President himself. It might in some cases even result in having a restricting influence on the conduct of operations. The recent beheading of an Indian soldier on the Line of Control in Jammu & Kashmir is also instructive. The news was all over the media almost immediately and then it spiralled into a major controversy: passions were frayed and the public opinion enraged. This led to cooling of various initiatives of normalising relations by both India and Pakistan. The heat generated was so much that it even invoked response from some outside powers urging restraint to be exercised. The Pakistanis backed off under pressure and there was easing of tensions. This spectacular power of cyber space has been exploited by the opinion makers and the business houses quite effectively to increase their visibility and to enhance business interests. Increasingly the various government agencies are utilising social networking sites to interact with the public at large. It can also be exploited as effectively by the Military to conduct perception management operations across the spectrum of conflict.

The greatest advantage of social media for perception management is its reach and speed. It can reach even an audience that is otherwise difficult to reach using conventional means. The medium is interactive and swaying. It allows dynamic modifications of the themes to shape the environment based on the feedback. Due to its interactive nature, it can act as an important tool to gauge the effects of the perception management endeavours. There are systemic opportunities and accepted practices to assume pseudo identities and thus remain somewhat anonymous. It might be a good idea to create pages on popular social-media sites to interact with prospective candidates to join the service and guide them through the process. This would be useful as the service has various entry points at which the candidates join the service. It can cater to the requirements by creating different pages and timelines. Creation of events on social networks for special occasions like the Army Day, Vijay Divas etc. will increase visibility and allow the common people to interact with their military. It can become a powerful tool to provide an insight into various disaster management tasks the Army undertakes every year.

The separatists and terrorists in J&K and elsewhere very often use the Facebook, Twitter and other social media tools for propaganda and to spread anti-national canards. Terrorists groups operating in various parts of the country as well as Left Wing Extremists have been known to communicate and pass instructions using the social media. Their sympathisers create pages for

**Monitoring of the social media over time is a useful tool to gather information regarding various trends and undercurrents among the target audience in counter insurgency and terrorist situations.**

causes and events to create empathy and support. Monitoring of the social media over time is a useful tool to gather information regarding various trends and undercurrents among the target audience in counter insurgency and terrorist situations. Blogs and the social networking sites have a wealth of information that can be gathered from open sources. This activity requires personnel who have a flare for and expertise in handling social media. Since colossal data has to be sifted and analysed it correspondingly requires training of personnel and software support capable of trend analysis, collation and comparison. These techniques have been used elsewhere for charting trends of protests at different geographical locations and the content used in the new media to communicate by the inimical elements before or after an event.

Malware based cyber-attacks on the social networks are a reality that needs to be contented with. Specially crafted malware have been spread through social media allowing large scale attacks. Social network platforms have been used for bot recruiting and also for hiding the command and control infrastructure and related traffic. According to the IBM X-Force 2012 Mid-year Trend and Risk Report, “social networks have been the dominant targets of email phishing for more than two years, and drive-by downloads are becoming the principal method of infection.”<sup>4</sup> Cyber espionage by adopting fake identities and adopting other techniques are known practices that have been used on the social networks. These are serious and must be taken note of. Suitable safeguards and preventive actions become an imperative.

Recently, there was a discussion in one of the groups on popular networking site ‘LinkedIn’ on what was the group’s perception of the definition of cyber security? There were many responses but the one by Mr Rhett Greenhagen, one of the members of the group, was simple and striking. It read, “Honestly, to me, Cyber Security is a term used by someone who does not work in this industry, or someone who is on the outside looking in.” It simply conveys that there is nothing known as absolute security in the cyber space.

There is a necessity for the military to have a controlled access to the social media. However, prudent caution needs to be exercised while doing the same. Social media platforms are powerful assets that invariably have the possibility of

a large number of threats. Though serving military personnel are discouraged to join social networks, there is no restriction on family members and they use the same quite extensively. It is thus necessary to initiate both the serving personnel and their families on how to manage their exposure to social platforms.

## **Conclusion**

Emergence of new media has transformed warfare especially at the lower end of the spectrum. There has been steady movement from mass application of force to precision application and now to adaptive application. The people-centric approach and use of minimum essential force advocated by the Indian Army in conduct of counter insurgency operations now stands as a model for some of the more modern militaries. However, there is a need for responding to the new operational realities by understanding and exploiting the new media. This calls for creation of a dedicated task-force and support structures to undertake these operations in real time as the opportunities emerge both in peace and in combat situations.

---

Maj Gen **Umong Sethi** (Retd) is a defence analyst based in Delhi.

## **Notes**

1. War 2.0 Irregular Warfare in the Information Age, Thomas Rid & Marc Hecker, Pentagon Press 2010