Social Media: New Dimensions of Warfare

Lieutenant Colonel Akshat Upadhyay[@]

Abstract

This essay examines the features of social media platforms (SMPs) and their weaponisation by state and non-state actors alike. The author argues using a host of examples that the age of total war has diminished, if not obliterated completely. A state where every citizen is simultaneously a combatant and a target, a citizen's war, has been the norm ever since the end of the Cold War. Use of SMPs has exacerbated various fault lines within societies. This has been adequately exploited by actors in Low Intensity Conflict Operations (LICO). Examples such as Hong Kong and Inter–Services Public Relations (ISPR) during the Balakot crisis come to mind. Finally, the author suggests structural, organisational and doctrinal changes by analysing various doctrines, joint and service-specific, to ensure that the Indian Armed Forces are better prepared to take advantage of this extremely potent tool, and use it not only for defence but offensive action too.

Introduction

Social media, an umbrella term, is defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content. Enabling cheap, accessible and instant communication worldwide, social media has revolutionised the way people interact with each other. It is based on Web 2.0 which emphasises user generated content over state/ corporation based broadcast modes. The variety of content afforded and integration with number of smart devices implies that the same platform can be used to influence people devoid of any geographical inhibitions. This influence, when weaponised by nation states and non-state actors alike may render conventional warfare impracticable.

Shifting Paradigm of Warfare

War is a means to achieve a state's political objectives through the utilisation of military force. From Napoleon till the end of the Second World War, warfare was state-centric and 'total' i.e. involving the entire society. However, the advent of nuclear weapons and rapid decolonisation across Asia and Africa have made 'total' war less probable now. Massive societal, cultural, political and economic faultlines within the newly created countries have led to the rejuvenation of terrorism as a favoured method of conflict. We are now witnessing a 'war amongst people'[1], a war where civilians are the targets, objectives, and predominantly the opposing force. Social media, which comprises users, social media platforms (SMPs) and related infrastructure, by placing content creation, analysis and delivery into the hands of users along with providing a common platform for idea and ideologies, has brought warfare participation down to the level of ordinary citizens.

Attributes of Social Media

The Good. The main attributes of social media are accessibility (extremely low barriers of entry), speed (maximum impact, minimum time), anonymity (manipulation, fake news), high volume of data exchange (noise versus genuine content), and flat structure (common platform for minorities, radicals and extremists alike). An innovative use of social media has been the use of open source intelligence (OSINT) to uncover state complicity in terrorist acts. Activists mobilised people for Arab Spring and the current protests in Hong Kong using SMPs.[2]

The Bad. Use of social media exposes vulnerabilities of users (manipulation of news feed of 700,000 users - emotional contagion[3]), provides an unregulated environment (8chan and Christchurch and El Paso shootings), and enables rapidity of spreading panic (child kidnapping messages on WhatsApp and subsequent lynching of innocent people).

And the Ugly. Islamic State (IS) and Al Qaeda (AQ) have exploited SMPs for spreading their extremist ideologies[4], recruiting members, intimating the progress of their battles[5] and franchising their expertise down to individuals. SMPs have been supplemented by sensor based devices along with applications (apps) which merge physical, emotional and cognitive attributes of users to create what some analysts refer to as 'surveillance capitalism', mining of big data for generating revenues.[6] Combined with the emotional contagion effect, data from SMPs have been used by companies like Cambridge Analytica for influencing the results of the United States (US) presidential and many other elections and United Kingdom's Brexit campaign.[7]

Weaponisation of Social Media

Non-Viability of Warfare Generations. There have been attempts to categorise warfare into generations with defining characteristics, however, most ideas and technologies of these 'generations' bleed into one another rather than staying impermeable. This simply implies that despite conventional battles or inter-state rivalries being considered passé, they operate alongside SMPs and terrorism to give rise to complicated battlefield scenarios where information dominance will lead to an overwhelming edge. In most scenarios, the adversary aims to affect change in population's attitudes towards their host government to exacerbate existing faultlines and weaken the state from within, thereby precluding the need for major military confrontation. SMPs which are designed to collect and monetise massive data about their users are the best platforms to conduct these operations.

Russian Information Operations (IO) Efforts. Russia ran an extensive campaign to influence election results in the US. In an exhaustive study, where a total of 10.4 million tweets, 1100 YouTube videos, 116,000 Instagram posts, and 61,500 unique Facebook posts published by Russian Internet Research Agency (IRA) from 2015 through 2017 were analysed[8], a tenuous link was established between the Russian efforts and outcome of the election results. Also, Facebook's head of security in 2017 specifically pointed out the 'Unpublished Page Post Ads' feature that allowed for very specific targeting of audiences.[9] These ads were used to generate hostility towards certain ethnic groups and run a negative campaign against some candidates. Russia also used social media extensively to undermine the credibility of the Ukrainian government using hoaxes, fake news and integrating its mass media network with social media attacks.[10]

Pakistan IO during Balakot Crisis. Pakistan's Director General of Inter Services Public Relations (DG-ISPR) has used social media extensively as a weapon both against adversaries and citizens alike.[11]

The Balakot incident showcased attempts by ISPR to wage hybrid war (conventional and unconventional capabilities applied together) against India. Misinformation on the location of Balakot, number of terrorists killed in Indian airstrikes, number of captured Indian pilots and Pakistani downed pilots saturated SMPs, mostly in the form of bots and fake accounts. Attempts were also made to create/reinforce political divisions within India during the Balakot episode. Most of them were removed later by Facebook and Twitter. Edited videos of the captured pilot were circulated by ISPR to discredit the Indian government. ISPR also coordinated a number of columns by reputed Pakistani expatriates, floated and retweeted heavily, which put the focus on Pakistan's apparent magnanimous gesture of returning the pilot and painting the Indian state as aggressive.

Use of Social Media by Non State Actors. This article assumes a broad view of non-state actors, not limiting them to violent groups only. The major aims for non-state actors are recruitment, propagation of message and illegally overthrowing existing structures of governance. Cambridge Analytica, a 'big data' firm, boasted of 'supporting' around 100 electoral campaigns across five continents using SMPs.[12] IS live tweeted its war against the Iraq Army during its capture of Mosul in 2014.[13] Initially predominant on Twitter and Facebook, IS used a number of innovations to ensure that it captured global attention. It used trend hijacking / hashtag hijacking during Football World Cup, embedding beheading videos on trending World Cup hashtags on Twitter[14], used cross-sectional linking of SMP links and influenced a number of Westerners to join the Caliphate using a number of online 'influencers'. Once social media giants started shutting down IS accounts, it switched to 'adaptive cognitive networks', a technique wherein a number of inactive accounts are used as reserves, in case of main accounts being shut down or suspended. The reserve accounts are then repopulated with almost the same number of followers using retweets and messages. This is known as the 'DEER' approach i.e. Dissemination, Deletion (thwarted), Evolution, Expansion and Replenishment.[15] IS, AQ and other terrorist groups have now shifted to lesser known but heavily encrypted and unregulated platforms such as justpaste.it, dump.to, Telegram, Signal etc., the so-called 'black boxes' of IS propaganda. AQ even published a Do-it-Yourself (DIY) guide to making a bomb using ingredients from a home kitchen, in its English language magazine, Inspire.[16] Protestors across the world use SMPs to mobilise and challenge state authority in countries as diverse as India, China, US and Brazil.

Social Media and Low Intensity Conflict Operations (LICO)

With such diverse implementation, social media has proved to be a game changer in LICO, which are a series of conflicts in a long drawn 'people's war'. Here the most important actor is the ordinary citizen as he is the target, audience and the adversary. The war is for the hearts and minds and perception management trumps kinetic operations.

Use of Social Media by Non State Actors in LICO. Social media's use in LICO is devastating. It is used by non-state actors to conduct propaganda operations, using photos and videos shared on SMPs to create / reinforce negative perceptions of security forces, state authorities and institutions. It is also used to mobilise and plan operations, crowdsource funds for operations and most importantly, recruit members to the cause. In case of Jammu and Kashmir (J&K), *nasheeds* (religious songs) are used in videos of killed terrorists and floated on social media to influence the population while WhatsApp and other platforms are used to quickly congregate at an encounter site and block the operations of armed forces.

Use of Social Media by States in LICO. States can resort to either strategic communication (SC) or IO when dealing with adversaries in LICO. SC implies using pan government resources and processes and engaging key audiences to advance national interests using coordinated information, themes, actions in sync with other elements of national power. Here the term 'key audiences' refers to friendly, neutral and adversarial audience. The focus is exclusively on the cognitive domain. IO focuses on the physical, informational and cognitive domains of adversarial human and automated decision making. SC and IO make heavy use of social media but for different purposes. SC is used to send coordinated messages to the intended audience where one of the media is social media and intention is to engage and understand. IO is more offensive, where social media is used both, for countering propaganda and saturating the information space with noise in times of war / conflict. SC and IO can be applied in LICO simultaneously but have to be done by different actors, so as to maintain credibility of the messages.

Components of SC and IO. SC comprises enabling capacities such as public affairs (PA), psychological operations (PsyOps) and military diplomacy (MD).[17] It aims to balance physical actions with aspects of IO to focus on the cognitive aspect of key audiences. SC is conducted at the highest level i.e. the department handling foreign affairs. Military operations support SC. IO, on the other hand, consists of three major components: cyber infrastructure, electromagnetic spectrum operations and PsyOps. It is inherently a military operation that targets the physical, technical and cognitive domains of the adversary’s human and automated decision making processes i.e. the users and their networks. The aim is to influence, disrupt, corrupt or usurp. Capabilities used are in the open as well as covert domain. Social media forms part of PsyOps.

Indian Army and Social Media

Manipulation of Security Forces and Families. Security forces, particularly their families, are at heightened risks of being manipulated through social media. This manipulation broadly takes either of the two forms: divulging of classified information; coercing individuals to undertake operations within their host country.

Leakage of Classified Information. SMPs collect massive amounts of personal data on their users by continuously analysing what they post, time spent, their likes, comments, etc. This data is sold off to various commercial entities for use in targeted ads. SMPs are also merging with bio-sensor and audio enabled devices, such as smart assistants and fitness bands, to generate and collect additional data about their users. Sometimes this data is inadvertently leaked, as in the case of Strava, a jogging app, which revealed the location of American secret military bases in the public domain. A number of times companies employ artificial intelligence (AI) or humans to ‘listen’ to conversations of their users. All these are security hazards. Conversations involving locations and movement of formations can be easily captured by such devices.

Undertaking Operations against Host Country. Honey traps and entrapments are common methods through which state and non-state actors try to coerce and manipulate security forces, and their families, into conducting espionage or worse, sabotage. A number of themes, such as 'Referendum 2020', are being used to target specific demographics within the armed forces to sow discord. Targeting capabilities afforded by SMPs, primarily for commercial companies, can easily be exploited to push theme specific agendas. Chinese agents prowl job search SMPs, such as LinkedIn, to lure members of armed forces by pretending to be academicians or prospective employers. Prolonged usage of social media is leading to major disciplinary issues within the armed forces themselves.[18]

Social Media Hygiene. The best way for security forces, and their families, to keep themselves safe from inimical actors on SMPs is to follow a good social media and cyber hygiene. Basics such as not logging on to unprotected WiFi networks, disabling geotagging on mobiles, double checking the various permissions given to apps, periodically checking on the members of various groups within SMPs, switching off mobile data when not in use, should be followed. Every major and minor unit must appoint / train an individual within the unit, a 'social media advisor' who must perform informal checks on the mobile devices of families for loopholes and also advise them on the way forward.

Doctrinal and Structural Changes Required in Armed Forces

Understanding Armed Forces Doctrines. The latest 'Indian Army Land Warfare Doctrine 2018'[19] and the 'Joint Doctrine for Indian Armed Forces (JDIAF) 2017'[20] remain the only public resource available for analysing the intent, capability and capacity of armed forces to use social media as part of next generation warfare. India does not publish any defence white paper, neither has a concrete National Security Strategy (NSS) document yet. Though both JDIAF 2017 and Land Warfare Doctrine refer to social media, the focus is on a very narrow and conventional understanding, essentially as a platform for hosting violent content or for public relations (PR). The Land Warfare Doctrine lists utilising social media as part of PsyOps for 'Public Information (PI) and Perception Management (PM)', a term which has become obsolete. Similarly, JDIAF refers to use of social media as part of 'internal threats and challenges' for 'radicalisation of youth in some states'.[21] Both the doctrines, with their exclusive emphasis on traditional definitions and understanding of social media as inherently negative, still propound a territorial approach towards warfare.

Targeting the Cognitive Domain. Indian armed forces' offensive focus is effectively on the physical and to a degree, technical aspect of cyber warfare. The third, that is cognitive, still remains peripheral to operational plans. Cyber operations, as envisaged for war, are essentially for cyber network defence, exploitation and attack, focusing on the electromagnetic spectrum (EMS) and physical systems. Their effects are generally instant and can be verified by involved agencies. Cognitive changes, whenever affected, are difficult to gauge and require constant and long term monitoring. Their effects are also not very evident directly on the objects against which operations are conducted. Changes may be visible in the medium of on and offline communications. Minute variations in tone of messages on SMPs or garnering likes on subjects previously left untouched may indicate a cognitive shift. It must be stated that merely a cognitive shift is not the terminus. Due to the unpredictable nature of human thought process, this shift may just be the opposite of what is aimed at. So, cognitive shifts need to be monitored by specialists in armed forces who can detect these changes and design their themes or narratives continuously to intervene and apply mid-course corrections.

Doctrinal Changes Required. Doctrinal changes that need to be incorporated involve; *firstly* recognition of the increasing use of social media as force multiplier for forces; *secondly* use of influence operations to manage attitudes and behaviours of target population using social media; *thirdly* incorporation of all aspects of social media such as Open-source intelligence (OSINT), encryption and communication in operational plans of the formations; and *fourthly* use social media as part of strategic communication on the strategic and theatre level. Within the three Services, Additional Directorate General of Public Information (ADGPI) is mandated to carry out social media monitoring to dispel misinformation about the army. The Defence Intelligence Agency (DIA) also carries out social media monitoring but is under HQ Integrated Defence Staff (IDS). None of them is mandated to use social media as an offensive tool of IO.

Structural Changes Required. The tasks currently envisaged for Defence Cyber Agency (DCA) are EMS operations and cyber operations, two of three components of IO. However, there needs to be a third vertical that focuses on social media operations. The ‘how’ and ‘why’ will flow either from the NSS or Raksha Mantri’s Directives. The social media vertical must include three subsections: content creation, monitoring, and research and analysis. The content creation team will design broad themes and narratives as per the prevailing situation and strategic directives received from the government. The content monitoring team will apply social media analysis (SMA) tools to scan the various relevant SMPs for ‘flashpoints’ - any likely piece of information such as a comment, picture, video or news item, which has the potential to go ‘viral’ and is malafide in its intent. The research and analysis team will look for unregulated SMPs or message boards, scour the ‘Deep’ and ‘Dark’ web and create analysis reports, using relevant historical and cultural contexts, to feedback the other two teams. They will also act as advisors for the IO formations at the command level and below.

Cyber Command. DCA, which may later be reconfigured as Cyber Command (CYCOM) with creation of integrated theatre commands, will formulate region / fault line specific social media directives and disseminate them to the theatre commands’ IO directorates, to pass them on further to the field formations. The three Services will also maintain their respective PI directorates which, in conjunction with CYCOM, will act as part of SC of Ministry of External Affairs (MEA). All field formations will have integrated social media cells to convert the broad directives received from CYCOM into specific themes, monitor local pages on SMPs and input the information to their commander to enable him to create effective battle plans. This format will be more effective in the theatre command or Integrated Battle Group (IBG) concept as both are geographically tailored for particular terrains and adversaries and cognitive aspect of IO requires longevity and sustainability of the themes and narrative to make the target population more palatable to our operations.

Coordination with Various State Organs. Social Media Intervention Teams (SMITs) must be created at CYCOM / DCA and theatre command levels that respond to ‘wildcard’ events by either coordinating with SMPs to shut down accounts or intervene to prevent a hashtag from trending. Liaison with local law enforcement agencies (LEAs) in case of spotting extremist content and internet infrastructure providers may be resorted to by CYCOM. CYCOM may also establish an Artificial Intelligence (AI) / Machine Learning (ML) cell, in conjunction with Defence Research and Development Organisation (DRDO), to liaise with industry and academic experts on how to integrate AI / ML with social media 'Big Data' analysis. This will enable it to pick up threats and opportunities for exploitation much faster. CYCOM, through the National Cyber Security Coordinator (NCSC), can coordinate with National Investigative Agency (NIA), Intelligence Bureau (IB), Research & Analysis Wing (R&AW), Ministry of Home Affairs (MHA), Ministry of Defence (MoD), MEA and the signal intelligence (SIGINT) directorate of the DIA.

Conclusion

Social media, through its user generated content and instant communication, has changed the way warfare is being / will be waged. More innovations in terms of 'deepfake' videos[22], website morphing will test the credibility of the state as a whole, more so the armed forces, to find and fix the enemy. No more can any country declare 'we have won the war' so convincingly. It is imperative that the armed forces be trained and educated in the use of social media as an enabler, and also be aware of its use by vicious actors to create conditions of war or worse, fight a war without us even realising that it has begun.

Endnotes

[1] Smith, R. (2005). *The Utility of Force.* 2nd ed. New Delhi: PENGUIN BOOKS, pp.2-15.

[2] Wolfsfeld, G., Segev, E. and Sheafer, T. (2013). Social Media and the Arab Spring: Politics Comes First. *The International Journal of Press/Politics,* [online] 18(2), pp.115-137. Available at: http://ijpp.sagepub.com [Accessed 17 Aug. 2019].

[3] Sellinger, E. and Hartzog, W. (2015). Facebook's emotional contagion study and the ethical problem of co-opted iden-tity in mediated environments where users lack control. *Research Ethics,* [online] 12(1). Available at: https://journals.sagepub.com/doi/full/10.1177/1747016115579531 [Accessed 18 Aug. 2019].

[4] Upadhyay, A. (2017). Anatomy of Lone Wolf Terrorism: Special Emphasis on Countering Violent Extremism. 1st ed. NEW DELHI: KW Publishers.

[5] Brooking, E. and Singer, P. (2016). War Goes Viral. *The Atlantic,* [online] (November 2016). Available at:

https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/ [Accessed 18 Aug. 2019].

[6] Vaidhyanathan, S. (2018). Antisocial Media: How Facebook Disconnects Us and Undermines Democracy. 1st ed. Ox-ford University Press.

[7] *The Great Hack.* (2019). [film] Directed by K. Amer and J. Noujaim. Netflix.

[8] Thompson, N., Lapowsky, I. and Barrett, B. (2018). How Russian Trolls Used Meme Warfare to Divide America. [online] WIRED. Available at: https://www.wired.com/story/russia-ira-propaganda-senate-report/ [Accessed 24 Aug. 2019].

[9] Vaidhyanathan, S. (2018). Antisocial Media: How Facebook Disconnects Us and Undermines Democracy. 1st ed. Ox-ford University Press.

[10] Lange-Ionatamishvili, E. and Svetoka, S. (2015). Strategic Communications and Social Media in the Russia Ukraine conflict. Riga: NATO Cooperative Cyber Defence Centre of Excellence.

[11] Upadhyay, A. (2019). Decimating Democracy in 140 characters or less: Pakistan Army's Subjugation of State Institu-tions through Twitter. *Strategic Analysis,* [online] 43(2), pp.101-113. Available at: https://www.tandfonline.com/doi/full/10.1080/09700161.2019.1600823 [Accessed 20 Aug. 2019].

[12] BBC News. (2018). *The global reach of Cambridge Analytica.* [online] Available at: https://www.bbc.com/news/world-43476762 [Accessed 24 Aug. 2019].

[13] Brooking, E. and Singer, P. (2016). War Goes Viral. *The Atlantic,* [online] (November 2016). Available at: https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/ [Accessed 18 Aug. 2019].

[14] Upadhyay, A. (2017). Anatomy of Lone Wolf Terrorism: Special Emphasis on Countering Violent Extremism. 1st ed. NEW DELHI: KW Publishers.

[15] Network of Terror: How Daesh Uses Adaptive Social Networks to Spread its Message. (2015). 1st ed. [ebook] Riga: NATO Strategic Communication Centre of Excellence, pp.1-24. Available at: https://www.ceeol.com/search/gray-literature-detail?id=661319 [Accessed 24 Aug. 2019].

[16] Sarat-Saint Peter, H. (2019). “Make a Bomb in the Kitchen of Your Mom”: Jihadist Tactical Technical Communication and the Everyday Practice of Cooking. *Technical Communication Quarterly,* [online] 26(1), pp.76-91. Available at:

https://www.tandfonline.com/doi/abs/10.1080/10572252.2016.1275862 [Accessed 24 Aug. 2019].

[17] Department of Defense (2006). QDR Execution Roadmap for Strategic Communication. Washington DC: Department of Defense.

[18] Singh, R. (2017). *Kashmir: Army jawan kills Major who reprimanded him for using cellphone on duty.* [online] Hindu-stan Times. Available at: https://www.hindustantimes.com/india-news/indian-army-jawan-shoots-dead-major-after-officer-reprimands-him-for-using-cellphone-on-duty-in-kashmir/story [Accessed 25 Aug. 2019].

[19] Indian Army (2018). Indian Army Land Warfare Doctrine 2018. New Delhi: Indian Army.

[20] HQ Integrated Defence Staff (2017). *Joint Doctrine Indian Armed Forces.* New Delhi: Bharat Shakti.

[21] ibid.

[22] Chivers, T. (2019). *What do we do about deepfake video?.* [online] the Guardian. Available at: https://www.theguardian.com/technology/2019/jun/23/what-do-we-do-about-deepfake-video-ai-facebook [Accessed 25 Aug. 2019].

[@]**Lieutenant Colonel Akshat Upadhyay** got commissioned in Army Air Defence. He is a prolific writer and has written a number of papers and articles for national and international journals, magazines and newspapers. He is author of the book 'Coercive Diplomacy against Pakistan'. This is the edited version of the article which won the first prize for USI Gold Medal Essay Competition (Group B) 2019.

Journal of the United Service Institution of India, Vol. CL, No. 619, January-March 2020.