



# ISSUE BRIEF

No. 309

November 2021

## Interpreting the War of Attention: Impact of Social Media on the Armed Forces



**Colonel Gaurav Gupta** is a Former Senior Fellow at CLAWS. He is an alumnus of the National Defence Academy. He was commissioned into the Corps of Signals in December 1992. He has served in various appointments in the field of Telecomm and IT in all terrains of Indian Army. The officer also served at Army HQs in DGIS and at Army War College, Mhow, where he was responsible for management of IT and Cyber Security. His areas of interests are IT, Cyber Security and Information Warfare.



**Thejus Gireesh** is working as a Young Professional at the Vivekananda International Foundation, New Delhi. He graduated in Political Science (H) from the University of Delhi. He has previously worked with CLAWS, the United Services Institution of India, and the National Maritime Foundation. His research interests are focused on information warfare, maritime security, military studies and geopolitical issues.

### Introduction

*“Unsurprisingly, social media can be both the cause of and the solution to your organisational crisis. It’s an ally and an enemy at the same time”.*

—Nicole Matejic<sup>1</sup>

The ‘war of attention’ i.e. is a tug of war played between the social media companies and users to grab and ensure maximum attention towards its social applications. The social media companies with its interactive algorithms and vice versa the users remain keen to share their personal stories to a global audience. In the contemporary world, social media has become an essential component of our daily lives. Social media has enabled people to voice their opinions, shape perceptions, and connect with people across the world— amplifying their voices from ordinary people to national

### Key Points

- Many countries across the world have extensively used social media to conduct information warfare. Countries like US, Russia, China etc. uses social media as means to deceive, discredit, undermine and frustrate the adversary's local population, and other critical institutions.
- In the new information age, the armed forces have become an important stakeholder, both as security providers of a nation as well as individuals.
- The impact of social media would be intensely thrust upon the newer generation of recruits, young officers who are more 'tech-savvy' or who have led a more technologically adept lifestyle especially on social media platforms
- Adopting a lenient social media policy for all ranks is essential for a sound social media strategy.
- The current organisational structure that looks into the issues pertaining to social media, cyber policy planning at the apex level institutions are divided, which may affect the overall operational performance.



leaders. With the growing number of social media users, armed forces worldwide have also felt social media's impact either as a PR (Public Relations) front or for unofficial communications, or even for tracking news. As warfare have shifted from traditional to multi-domain encompassing electromagnetic, cyber, space, and so forth, a major battle of perceptions and opinions to 'condition' people's minds is being fought on the social media. Not long ago, with the Armenia- Azerbaijan conflict, the artful usage of social media to win the psychological battle ensured that the population shall to muster arms when desired by their respective countries and made the world realise the gravity of the situation.

The armed forces are finding themselves in a dilemma as their traditional and supposed 'more secured' means of communication such as letters and telephones are increasingly becoming redundant. The Indian Armed Forces are also facing the same dilemma as India represents one of the world's largest internet user markets.<sup>2</sup> The soldiers often live in isolation and in remote areas distant from the local population; in harsh atmospheric conditions that are characterised by strenuous physical and mental conditions —social media can be solace in gloomy times for the soldiers. For the armed forces, social media is becoming an important means to communicate with the general public that is as an organisation to promote its roles within the society, attract new recruits, and as a platform for broadcasting official information.

The forces in the Western world are embracing social media to bring in human touch and are trying to connect their respective organisations to a bigger audience for greater accessibility. Just as the armed forces are gradually opening up to this new medium, questions on the effective use of social media by the armed forces, the psychological reaction to social media and how should the armed forces personnel use social media without hampering the ethos and secretive nature of the armed forces are yet to be answered. The paper shall examine how social media affects the armed forces, discussing how to leverage social media effectively for better PR and harness social media. The paper has looked into how other forces across the globe have dealt with their social media policies and shall bring out some vital issues faced by the armed forces in respect to social media. Finally, it provide policy recommendations to effectively set up a social media strategy for the armed forces and its personnel.

### **The Strategic Realm**

Many countries across the world have extensively used social media to conduct information warfare. Countries like US, Russia, China etc. uses social media as means to deceive, discredit, undermine and frustrate the adversary's local population, and other critical



institutions. These countries have also given such activities an institutional framework and inculcated doctrines into their cyber and information operational capabilities. Russia sees its cyber domains more inclusively, which includes information warfare, psychological and electronic warfare within a single framework.<sup>3</sup> The Russian Military Doctrine of 2010, in regards to utilising information warfare necessitates “the prior implementation of measures of information warfare in order to achieve political objectives without the utilisation of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilisation of military force”.<sup>4</sup> Russia’s central intelligence organisation (GRU) is entrusted with the conduct of external operations, which includes cyber, information, and electronic operations, whereas the FSB conducts domestic surveillance along with Russia’s Foreign Intelligence Service (SVR)<sup>5</sup>. The sophisticated Russian meddling of the 2016 US presidential elections is an important example of Russian information warfare campaigns.<sup>6</sup> Similarly, such extensive use of social media platforms to conduct operations was also witnessed during the Russian annexation of Crimea wherein social media platforms were extensively used to influence the local population, spread fake news and rumours through social media.<sup>7</sup>

With the creation of the Strategic Support Force (SSF), China has created a robust military structure that looks upon the conduct of operations in cyber, information, psychological, and space domains in order to achieve ‘strategic commanding heights’ for the PLA.<sup>8</sup> The 2015, Chinese Defense White Paper also calls for ‘winning informationised local wars’.<sup>9</sup> This showcases that China considers controlling the flow of information to be as crucial as controlling a maritime chokepoint or ensuring air dominance in the battlefield.<sup>10</sup> The Chinese protect their internet ecosystem, popularly known as the ‘Great Firewall’. They restrict most of the popular western origin social media applications such as Facebook, Google, Yahoo, YouTube, etc. At the military level, the US has established a military command for dealing with cyber, information and electronic warfare, i.e., the US Cyber Command (US CYBERCOM). Although CYBERCOM shares the information operations with other US military commands yet CYBERCOM is not the primary command for the conduct of cyber operations.<sup>11</sup>

Unlike in the past, where the government could control domestic propaganda, social media platforms have opened a new realm wherein the domains are subject to incessant contestation, which involve the active presence of the adversaries within the internet trying to influence the people’s minds. As the traditional notions of warfare dynamically change, the social media sphere is likely to become a highly contested ‘grey zone’ with states engaging each other indirectly without firing a shot or moving into a full-blown war. Chaveso Cook and

Liam Collins rightly state that “The erosion of global borders is inversely proportional to the growth in internet usage. Contemporary life has a ubiquitous digital component. Increasingly, people around the globe log into a thriving online society that mirrors the physical community. Therefore, cyberspace and its influence have undoubtedly shaped all interactions, up to and including warfare, and technology has increased options for the antagonist as much as it has for the protagonist. Those that “seize the key terrain of social-media exploitation will have strategic military advantage”.<sup>12</sup>

In the strategic realm, India also experienced such operations. In February 2019, post the Pulwama attack and the Balakot airstrike, tensions escalated between India and Pakistan. , as the Indian Air Force undertook an aerial strike into Pakistan occupied Jammu and Kashmir. As a reaction, Pakistan also launched its failed counterstrike, which ensued in an aerial battle between the two Air Forces.<sup>13</sup> As the two-armed forces were engaged in a confrontation, a similar battlefield was being moulded in the realm of social media— the aerial battle’s visuals and the captured IAF pilot’s footages Both side of the borders were being widely viewed and shared on social media platforms. Later these visuals were reshared by television channels which doubled the penetration of visuals into the population.<sup>14</sup>

One of the forefronts of Pakistan’s information warfare campaign is executed under the aegis of the its Inter-Services Public Relations (ISPR), which is under the command of a Major General rank officer.<sup>15</sup> This organisation has constantly been able to weaponise social media to spread propaganda and conduct influence and trolling operations.

The recent Galwan standoff with China in May 2020 is one of the prominent examples of weaponisation of social media. During the standoffs, social media was extensively used by certain permitted social media personalities and media organisations of China to wage inflammatory and psychological operations against India. A prominent example of the same was when the Global times released a video commemorating the “Galwan Martyrs”<sup>16</sup> (Figure 1)<sup>17</sup> or the video released by proxy handles of China in regards to the Galwan clash. These actions were in perfect sync with



Figure 1: A Screenshot from a video on Galwan Clash shared in Chinese social media. Reshared by Ananth Krishnan on twitter. The time and date of the video remains uncertain.



the China's 'Three Warfares Approach' (3Ws),<sup>18</sup> that aims to control the narrative within China as well as to dissuade the adversary through the usage of extensive legal, psychological and media operations, thereby broadening the realms of conflict to achieve their national interests without resorting to a full-fledged war.<sup>19</sup> Such actions therefore showcases the effective usage of social media in a strategic landscape, and it is deemed to continue into the future with more enhanced levels of sophistication. Even as there was no presence of media where the conflicts took place, it is ascertained that the visuals of the clashes were taken and uploaded by troops posted in those areas and later hyped up in social media and media outlets, thereby explaining the reach of social media in conflict zones.

### **The Growth of Social Media Platforms**

Social media platforms in the recent decade have witnessed a massive boom in usage, especially after the COVID-19 pandemic.<sup>20</sup> As technologies developed over time, with the advent of telephones in the 19th century to the present age of smartphones, it ensured connectivity between people through all means except physical presence. By 2018, Facebook recorded over 2.26 billion users worldwide, most belonging to the age group of 18 to 47 years.<sup>21</sup> On the same lines, India in 2021 alone had over 320 million users.<sup>22</sup> Apart from social media being a mode for connectivity and communication among people across the world, social media has had substantial socio-political impacts from mobilising people for various causes to pressurising governments on many of its policies. Even the governments have been using social media aggressively to establish a direct connection with its citizens.

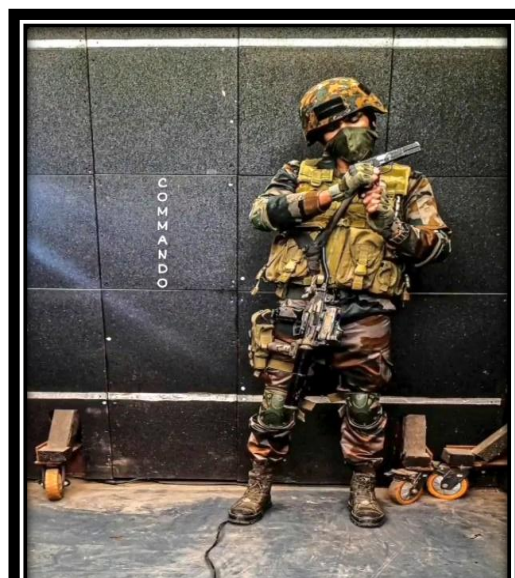
In the new information age, the armed forces have become an important stakeholder, both as security providers of a nation as well as individuals. With the means of communication evolving at an unprecedented scale, embracing social media as a tool for communication as well as addressing the threats posed by social media enabled hyper-connectivity is essential. During the 19<sup>th</sup> century, with the advent of telephones and telegrams along with printed materials, the armed forces were able to maintain checks and balances institutionally through different means such as availing telephone and postal facilities for its troops or by controlled information sharing among its troops in the forms of pre-approved magazines and so forth.

Presently, India, with its biggest digitisation drives — the 'Digital India' initiative<sup>23</sup> aims to promote digital literacy, digitisation of government, schemes and services and increasing internet connectivity in India. As a result, over 500 million people in India now own a



smartphone in which over 77 percent have an active presence online.<sup>24</sup> Therefore, with smartphones now offering better accessibility than a personal computer, accessing social media platforms through smartphones has become convenient even at the most remote and far-flung places.

***The psyche behind the use of social media.*** At a cognitive level, social media has had a tremendous impact on the neurological and psychological aspects of humans. Professor Sinan Aral in his book *The Hype Machine* evidently argues that social media is designed in a peculiar manner through which it takes advantage of the human psychological and neuro-physiological requirements such as socialisation, belonging, and social approval.<sup>25</sup> Studies suggest that receiving a 'like' in images or videos in social media platforms led to neural response in the Ventr Tegmental Area (VTA), getting a reward equivalent to gaining monetary terms or social situations.<sup>26</sup> The VTA is responsible for identifying rewards and increments in social statuses. Therefore, when the VTA identifies a similar response to receiving a like on social media platforms, it releases a dopamine, making human reactions such as excitement, joy, and exhilaration.<sup>27</sup> In an interview, the founding President of Facebook, Sean Parker stated that "How do we consume as much of your time and conscious attention as possible and that means that we need to sort of give you a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever. And that's going to get you to contribute more content, and that's going to get you ... more likes and comments. It is a social-validation feedback loop, exactly the kind of thing that a hacker like myself would come up with, because you're exploiting a vulnerability in human psychology".<sup>28</sup>



**Figure 2: A paratrooper with his Browning Hi-Power Pistol & IWI Micro UZI Machine Pistol & MEPRO MOR Sight, Suppressor**









effectiveness, and exploring social media data as a measure of audience reactions to relevant army information.

- China.** The increasing use of social media websites by young people in China and PLA has been changing the way news is consumed by the public. China constitutes the world's biggest social media market, but with no access to websites like Twitter, Facebook and YouTube—most people can only use domestic social media sites such as Weibo, Renren and YouKu.<sup>35</sup> For many, these sites are not just their main source of news—they are in fact sites to organise protests and put forth the people's own versions of events. Base 311, a PLASSF (People's Liberation Army Strategic Support Force) unit, is at the forefront of applied psychological operations and propaganda directed against other countries and functions as an operational PLA political warfare command. A 2018 report<sup>36</sup> foresaw that the SSF's fusion of cyber and psychological warfare capabilities could build new synergies between disparate capabilities that enable specific types of strategic information operations missions expected to be decisive in future wars.
- The European Union.** Social media is utilised at the international level to boost the reputation of the armed forces and to communicate the strategic narrative in an effort to win the increasingly important 'battle for hearts and minds'. At the national level, social media is used, for example, as a tool for recruitment and to create societal engagement for the armed forces. At the same time, social media poses challenges to the armed forces as information gets more difficult to control and transparency increases. This may lead to harmful effects in at least two ways. *First*, as the distribution of information conditions the distribution of authority, the command may be tempted to control more of the subordinates' activities, leading to micromanagement in international operations. *Second*, the distribution of information may expose soldiers to increased risk. Risk, in this regard, refers to "the possibility that human actions or events lead to consequences that affect aspects of what humans' value". More specifically, the unpredictable and uncontrollable features of social media along with the speed that information spreads and travels within these arrangements mean that "emerging information can reconfigure (continuously) political and public perceptions of defence activities in a manner that is detrimental to strategic and institutional (military) objectives". Social media use thus puts forth risk to security and to reputation that might affect armed forces' activity or relate to classified, operational, controversial, or political matters. Convergence/divergence among EU armed forces' views and use of social media is vital for successful

multinational military interventions, since lack of convergence among participating countries will pose problems for multinational collaboration and coordination. A study based on EU member states' armed forces' use of social media in areas of deployment shows that armed forces in general embrace social media as an opportunity more than they emphasise the risks.<sup>37</sup>

- **Australia.** The Australian Defence Force (ADF) increasingly relies on social media platforms, such as Facebook, for information and support. Private Facebook groups, has been created to facilitate discussion between ADF partners, as well as individual social media pages has been created where sensitive information is shared. The ADF currently has no resources specifically targeted to families regarding safe social media use. The approach taken by the ADF appears to focus on training the serving member in social media safety and then placing the onus on the member to share this information with his or her family. ADF members are provided with security briefings about social media as part of their annual mandatory awareness training. In an assessment of this training, a report by Patterson suggests that, there is "lack of training and an overt reliance on terms such as 'common sense'".<sup>38</sup> In addition to facilitating connections with friends, family and networks, ADF members find social media useful for communicating with their partners, especially during deployments.
- **Canada.** The current use of social networking in the Canadian Armed Forces is very limited in comparison to the capabilities of social networking that are being taken advantage in other industries and could benefit the Primary Reserve Force. The number of social media applications in the Canadian Armed Forces, although apparently lagging behind private business applications, is on the rise. However, the current use is primarily as a public affairs tool providing a type of an online scrapbook or to provide messages to the general public on the activities and achievements of the Canadian Armed Forces. Many units and formations have social media sites that they use to advertise and shares photos and stories of current or past events. However, there is an apparent reluctance to use social media for any formal communications with reservists. Overall, the Canadian Armed Forces is very involved in the use of social media as public affairs tool. The Canadian Armed Forces use social media primarily to communicate with the general public, and provide an online scrapbook for members, but does not take advantage of the ability to communicate with members for current and future training or administration.<sup>39</sup>
- **Russia.** Russia's Parliament has voted to ban soldiers from using smartphones while on duty, after their social media usage raised issues of national security. The bill forbids military personnel from using a phone with the ability to take pictures, record

videos and access the internet. Soldiers also cannot write about the military or talk to journalists. Phones with basic calling and messaging facilities could still be used, but tablets and laptops are also subjected to the new ban. However, the social media accounts used by soldiers has allowed open-source journalism sites like Belling cat to have access to sensitive military activity by undertaken by the Russian Forces. The bill is remains to be considered by the upper house of the Parliament, the Federation Council, before being signed into law by President Vladimir Putin. In recent years, social media posts by servicemen have revealed Russia's military presence in eastern Ukraine and Syria, sometimes contradicting the government's official claim of not having troops there.<sup>40</sup>

### **The Impact of social media on the Indian Armed Forces and the Army**

- **Security Threats.** The presence of service personnel on social media shall come with its own security challenges. As soldiers become more active on, social media platforms, there is a possibility that small pieces of information, posted on social media platforms, can be collated by adversaries to know the personnel's near-real-time whereabouts and this may jeopardise the security situation. The images and videos posted on social media by personnel are permanent and rarely gets erased from the internet. These images can also be traced through geo-tagging, analysing the metadata and also by identifying the physical features in the image or video. The images and videos can also reveal operational details regarding location, personnel, movements and so forth, thereby threatening operational security. These threats can be detrimental, especially when troops are posted in hostile or field locations. The information posted by personnel on social media can also be used to distort information by the adversaries for their advantage.
- **Information Espionage.** 'Honey Trapping' remains one of the oldest tools in the domain of information espionage. Honey Trapping basically works by enticing informers to give up information by fraternising with the opposite sex. Several cases of honey trapping have been found in India, such as in March 2021, an Army Jawan posted in Sikkim, while on leave, was arrested by the Rajasthan police for allegedly leaking confidential information to Pakistan through Facebook.<sup>41</sup> The leak of sensitive information is detrimental to national security and social media as a medium is often the cheapest and the most convenient tool for adversaries to extract information.
- **The Political impact.** A key challenge that lies ahead of the forces is the political impact of troops using social media. Politics and issues surrounding it are often very

personal and sometimes highly controversial. According to the Army Act 1950<sup>42</sup> - officers and other ranks of the armed forces are prohibited from airing their political views or participating in political functions. With millions of people present in social media applications, any opinion, or a statement by a serving member of the forces can be construed as political and, therefore, can cause harm to the overall image of the armed forces. For example, during the recent farmer's protest in January 2021, a soldier in uniform was found protesting at the site with the farmers<sup>43</sup>. Social media can also be used as a weapon for polarisation of the troops through targeted posting and advertisements on social media applications. Social media can also become a tool to create unrest among the troops as information spreads quickly in social media. During the investigation of US Capitol Riots, it was observed that in every five defendants, one had previously served in the US Armed Forces as also some of them were serving as US National Guard and Reservists.<sup>44</sup> However, their participation and airing of their views on social media platforms had severely impacted the image of the US Armed Forces.

- **Anonymity and Discontent.** Social media offers great deal of anonymity to their users. This anonymity can also be termed as a double-edged sword— *firstly* as anonymity allows the user a great deal of privacy to user from divulging private information. Secondly, anonymity can be used as a medium to to conduct bullying, raise discontent against the organisation, and conduct illegal activities online. Although, service members are restricted from raising issues and discontent on the social media, however, there have been cases, wherein social media was used to raise one's dissatisfaction; for example, a BSF constable posted a video on Facebook pertaining to the bad quality of food and alleged the senior officers of corruption. His video became viral in no time.<sup>45</sup> Such instances may drastically change the public perception of the forces. since such instances and controversies can quickly become 'viral' or spread fast in social media. Therefore, monitoring and addressing such instances in a time-bound manner may be critical to addressing this challenge. Using anonymity as a tool users, can also leak critical operational data without any attribution.
- **Effect on the mental health of Soldiers.** Karl Marx once said, "*Religion is the opium of the masses*" if so, then in the modern world, social media is increasingly becoming the new '*opium*' of the masses that affects all individuals one way or the other. As social media has grown over time, it has become more convenient to remain connected with family and friends, at convenience. However, this accessibility has come at a cost as troops are expected to stay away from their families in remote





locations without contact for days. The advent of social media has brought in regular communication with friends and family at an individual's time and choice. With the communication gap rapidly decreasing, it has also brought domestic issues into the minds of the service personnel, which often directly or indirectly affects troop performance. Social media has become a reason for increased anxiety among troops when something goes wrong back in their homes or when serving at high tension areas such as in CI/CT operations or in field postings.<sup>46</sup> Also, as soldiers spend their time in social isolation<sup>47</sup> in remote areas, they remain more occupied with their smartphones. These smartphones may be utilised for a variety of purposes such as gaming and entertainment, but smartphones have been found out as the primary means to use social media<sup>48</sup>. It and it has been found that the usage of social media applications. addiction to social media applications.<sup>49</sup> Also, The mental health of service personnel can also be affected if they face online bullying or are entrapped in online scams.

- **The Policy Perception Gap.** There is a significant policy gap between the establishment and the actual workings of social media. The social media policy is not updated regularly to address the problems arising out of social media. There is a need for a better and inclusive social media policy that incorporates optimum usage of social media by the forces. instead of tightly regulating since the service members can be adept at finding alternative means to use social media when tightly regulated.
- **Gap in Social Media Education.** As the power of social media platforms delves deeper into the cities and remotest areas in India, more and more people will rely on it to get news, banking, and other services. On one hand, the usage is growing and on the other hand the awareness of how to use social media optimally and responsibly is decreasing. Although social media applications are user-friendly and easier to use by nature, the consequences of the wrong usage of social media or its pitfalls are not commonly known among the troops. Also, as a majority of our troops come from remote villages and less educational backgrounds - it becomes necessary to train and educate the soldiers on how to use social media platforms. A simple tweet or a post on social media applications by service members can be 'misinterpreted' in many ways and hence create problems for the forces at large, that can be a cause for bad publicity for the forces among the general public or become a cause of concern for the leadership. If proper education regarding social media platforms is not provided to the troops, they may remain vulnerable to information leaks, a stolen identity, false fraternisation, etc.

- **Civil Violations.** As service personnel increasingly use social media, the challenge to deal with the breaking of domestic laws may come more into the limelight. The unauthorised use of certain audio-visuals in the internet by service members may constitute to copyright violation. Another important challenge is Privacy infringement, wherein user's personal details such as images, videos, and information are compromised on social media platforms by individuals or organisations. Social media platforms are often a lively place where intense debates and arguments take place. In such a scenario, an individual may make a false statement or make a statement that affects the reputation of an individual or an institution leading to defamation. Defamation charges are serious and may impede fines and jail time even if such statements are made in the cyber domain. Such civil violations poses significant challenges to the armed forces.

## Recommendations and Way Forward

*“The world is full of things more powerful than us. But if you know how to catch a ride, you can go places”.*

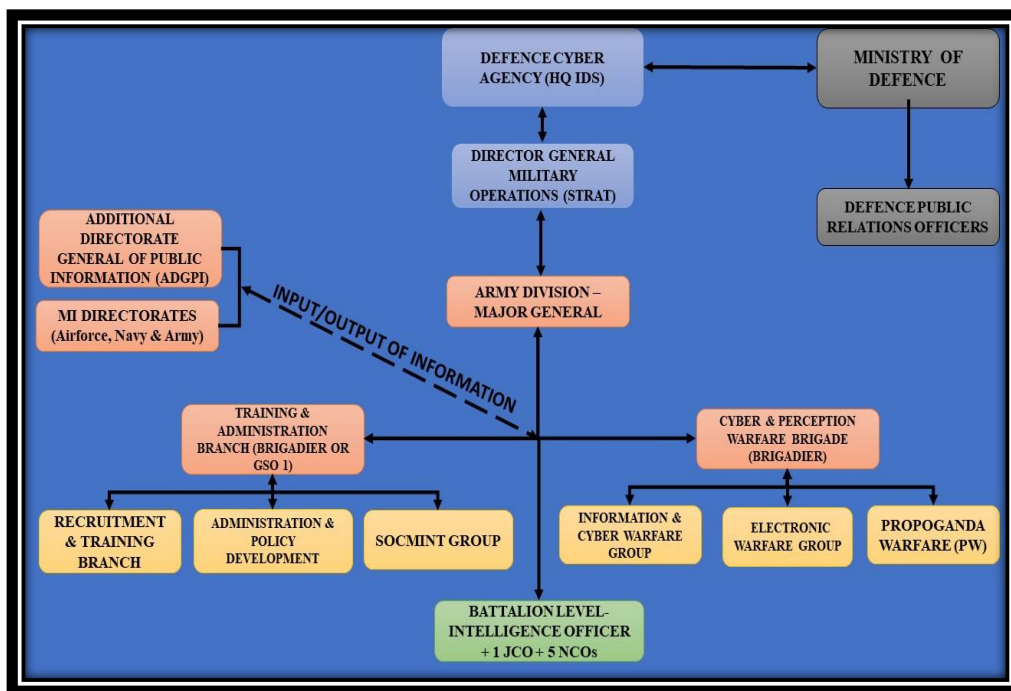
—Neal Stephenson<sup>50</sup>

Social media is a part of the greater cyber realm. Social media inhibits the properties necessary to conduct offensive and defensive cyber operations, intelligence gathering, information warfare, propaganda warfare, etc. Therefore, the recommendations shall contain a roadmap towards improving the existing social media policy as well as enhancing cyber domain capabilities. At places, they would be written interchangeably since social media forms an essential aspect of the cyber realm and if activities on social media are to improve, they would also require holistic revamping of the cyber architecture.

- **Internal Survey and Pilot Project.** The challenges and opportunities that social media presents to the world's armed forces are predominantly new. Many nations across the world have tried and tested their own responses to social media. However, an important point that needs to be addressed is that of the geopolitical situation, and the region where the forces conduct their operations. Social media will need to be dealt with in a particular way that fits our own tailor-made requirements. Therefore, a pilot project is essential to find out the root causes of social media's challenges on the armed forces. An internal survey consisting of the following points but not limited to such as the number of service personnel using social media, preferred applications, the brand of smartphones, consumption time and so forth

shall give the policymakers enough data to create a policy that optimally utilises the power of social media for the institution and its personnel. It is also beneficial to update the data from time to time. Therefore, a survey needs to be done periodically to remain cognisant to the newer dynamics that is relevant to the data, which may contribute towards updating the existing social media policy by acknowledging the 'hits and misses' of the previous policy. Finally, once the data is corroborated, a good way to assess different kinds of strategies would be to initiate a localised pilot project at the unit/brigade level for personnel based, corps/command level projects to assess the different strategies at the national level to assess the real-time impact of social media on the armed forces.

**Figure 4: The new proposed command structure. Author's own illustration**



- **Need for a Chain of Command.** For any effective operation in the cyber domain, there needs to be a clear chain of command that ensures adequate attention is provided to a particular operation, and social media is not any different. Operations on social media may be considered as part of propaganda, information, cyber, or intelligence operations. Therefore, they require a substantive organisational structure. There needs to be a single apex level organisation that looks into the operational and policy aspects relating to social media and the cyber domains. The current organisational structure that looks into the issues pertaining to social media,

cyber policy planning at the apex level institutions are divided, which may affect the overall operational performance. Therefore, to resolve this challenge, monitoring social media should be done at the brigade level. Collection and data processing on social media accounts could be done at the battalion level to ensure efficiency. At the battalion level, the commanding officer, Intelligence officer and JCOs, shall ensure that the policies are implemented, monitored and minor cases resolved at the lower levels. Another possibility is to create a dedicated Social Media Intelligence Team at the battalion level to assist operations and gather intelligence at a local level. We propose Cyber ISR (Intelligence, Surveillance and Reconnaissance) Division composed of specialised units and headed by a Major General at the higher structures. These changes in the organisational structure shall help to monitor, plan and operate in the social media and in the cyber domain as a whole (**Figure 4**).

- **Brigades for Social Media Offensive and Defensive Operations.** A similar model that can be adapted for Indian conditions is the United Kingdom's 77th brigade.<sup>51</sup> Composed of both reserve and permanent personnel specialised in information warfare domains, these brigades shall conduct Information activity, outreach, digital operations, media communications and so forth. For the Indian Army, such Brigades shall consist of (but not limited to) public perception, cyber media, electronic warfare, propaganda warfare, information warfare units. This division may report to the Director General Military Operations (Strategy) and maybe supervised by the Defence Cyber Agency under Headquarters Integrated Defence Staff to synergise the efforts between all the three services. The following brigade may consist of specialised regiment and TA (Territorial Army) battalions with officers and other ranks specifically looking into social media and cyber domains; the TA strength comprising civilian expertise in social media analytics, publicity, and Social media Intelligence (SOCMINT).<sup>52</sup> The members of the brigade may be deployed at various levels in the Army, such as in the brigade or unit levels, to conduct operations alongside troops on the ground or be attached at corps/ command levels to work in a strategic landscape.



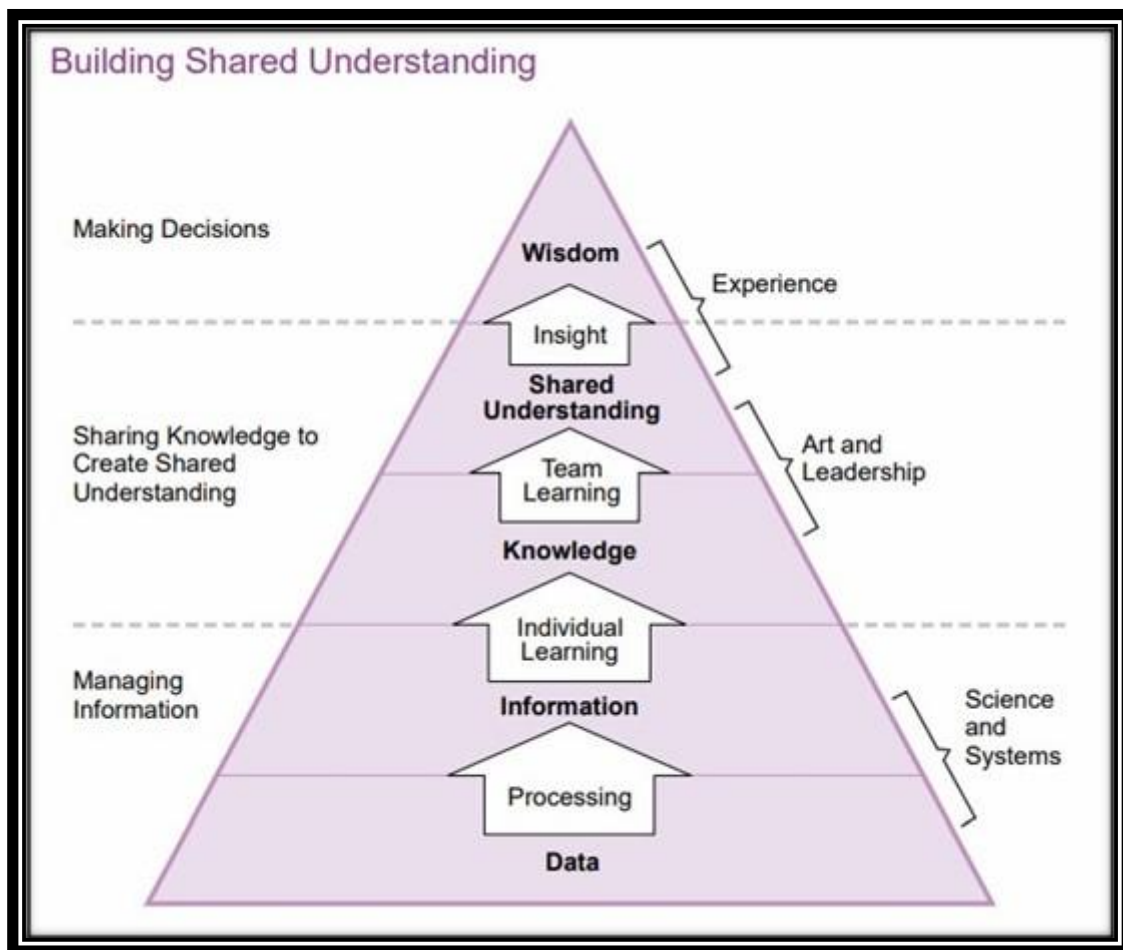


Figure 5: Building shared understanding of information<sup>53</sup>

- **Cadre Creation and Management.** As the nature of warfare in the modern world have become more complex and dynamic, so are the areas of social media and cyber domains. These domains require specialists to optimally leverage situations in social media domains and cyber domains such as Culture Specialists, Social Media Analysts, White Hat Hackers, Open-source Intelligence Analysts, Media Experts, Cyber Security Specialists, etc. An important aspect with regards to cadre management is that the serving officers and men need to be trained explicitly towards these domains, and these service personnel should not serve on a tenure basis to ensure field specialisation. Integration of TA battalions for these roles with domain specialists recruited from civilian backgrounds shall be an advantage. As the social media and cyber domains remain dynamic in nature, it shall allow new thought process to be included, and finally, the service retention for these service personnel will be more financially viable for the organisation. For other



services that may not host TA battalions, hiring industry professionals from civilian backgrounds after thorough security checks and clearances can be one consolidated solution **(Figure 5)**.

- **Bureaucracy and Synergy.** One of the biggest challenges in conducting a successful operation or implementing a policy is bureaucracy's slow nature. As social media and the cyber realms are dynamic and often require time-sensitive actions to resolve the challenges, an efficient and time-bound bureaucracy will be of great advantage to any organisation, as the decision-making time would be reduced, accountability will increase, and finally, operational performance would be enhanced. Another important aspect of improving organisational practices is enhancing synergy between the services. In a multi-domain battle scenario, every aspect of warfare remains critical to winning a battle. In the new age, after deployment in a region, maintaining a positive narrative regarding our forces among the population is essential as also to discredit, disorientate and frustrate the adversary through conventional and non-conventional means. Therefore, synergy between the different services is essential for successful deployment and operations. Social media can be a means to engage with the local population and gather intelligence regarding the adversary. In doing so, cross-service rivalry, lack of synergy, and stovepipe decision-making can significantly effect operational performance in an area. Therefore, to increase synergy, just as personnel are posted at the Defence Cyber Agency (DCA) at the apex level, cross-service personnel from the Army, Navy and Air force are necessary at the social media and cyber policy and operational levels.
- **Educational Programs.** Educational programs are one of the most important ways to mitigate the challenges that emerge from the social media domain. Service personnel needs to be trained periodically to optimise their use of social media applications without comprising operational or individual security. A way to incorporate social media education within the structure of the forces is to institutionalise the training methods and courses for the service personnel. This will enable a long-term understanding of social media platforms as well as the cyber domains. As digital footprints can become traceable by adversaries, service personnel needs to be given to given courses such as digital signature awareness training.<sup>54</sup> Such training must be periodic and should contain best practices in line with the social media strategy of the Army or armed forces. These programs must be conducted

across all branches, directorates and establishments of the armed forces, thereby incorporating all service personnel. The services should conduct professional social media and cyber courses for its personnel. The services must assess, develop and integrate talents within service personnel such as photographers, content writers, social media intelligence analysts to improve the public perception of the forces. These talents can be utilised to create a digitalised version of the Sainik Samachar to serve as morale boosters for the troops.

- ***Lenient Policy and Engagement.*** Adopting a lenient social media policy for all ranks is essential towards a sound social media strategy. In the armed forces, social media has integrated within the ranks; blanket ban or tight restriction on social media may not be fruitful. Therefore, a lenient policy may incorporate allowing service personnel to use social media on a condition that the personnel discloses/inform their making of social media accounts at the appropriate levels. Vetting of the information posted by personnel at the battalion levels can be a possibility considering other factors such as restrictions in stages in lieu with their area of posting such as in field, semi-field or peace postings. Individual pictures in uniform without rank may only be posted on social media after clearance from the unit Intelligence officer or from the appropriate Intelligence group within the unit so that there is no threat to operational security. To attract more recruitment, ensuring the availability of good footage for outreach, and increase accessibility to the public, an alternate content generation model can be adopted. This is by collaborating with media organisations that cover armed forces through shared copyrights over visuals taken by media channels. This can help in generating new content for the armed forces. The social media handles of the armed forces may also look into social trends that are good for the society and induce patriotism among the masses in social media with interactive images and videos to boost public perception of the social media handles. Social media can also be a great tool for military families and military leaders to acknowledge and encourage the achievements of their personnel and families. The social media engagement at Exercise Hamel conducted by the Australian Army in 2016 is a good example of proactive social media usage by the armed forces.
- ***Development of Indigenous Social Media Platforms.*** Nowadays, for the users, there are plenty of options to choose from when it comes to social







## End Notes

<sup>1</sup> Brigadier Mick Ryan et al., 'Social Media in the Military: Opportunities, Perils and a Safe Middle Path', *Grounded Curiosity* (blog), 20 August 2016, Accessed 03 July 2021 <https://groundedcuriosity.com/social-media-in-the-military-opportunities-perils-and-a-safe-middle-path/>.

<sup>2</sup> "Social Media Landscape, Demographics and Digital Ad Spend in India." Sannam S4, January 5, 2021. Accessed on 19 March 2021 <https://sannams4.com/digital-and-social-media-landscape-in-india/>.

<sup>3</sup> Grzegorzewski, Mark, and Christopher Marsh. "Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition." Modern War Institute, March 25, 2021. Accessed on 10<sup>th</sup> April 2021 <https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/>.

<sup>4</sup> Connell, Micheal, and Sarah Vogler. Rep. Russia's Approach to Cyber Warfare. CNA, March 2017. Accessed on 10<sup>th</sup> April 2021 [https://www.cna.org/cna\\_files/pdf/DOP-2016-U-014231-1Rev.pdf](https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf).

<sup>5</sup> Ibid.

<sup>6</sup> Office of the Director of National Intelligence. Assessing Russian Activities and Intentions in Recent US Elections. Rep. no. ICA 2017-01D. National Intelligence Council, Government of the United States of America, 06 Jan. 2017. Accessed on 10<sup>th</sup> April 2021. <https://apps.washingtonpost.com/g/documents/national/read-the-declassified-report-on-russian-interference-in-the-us-election/2433/&gt;>.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign

<sup>7</sup> Rep. Combined Analysis Russian Information Campaign Against The Ukrainian State And Defence Force. NATO STRATCOM Centre of Excellence, February 2017. Accessed on 10<sup>th</sup> April 2021 [https://www.researchgate.net/publication/314755402\\_Russian\\_Information\\_Campaign\\_against\\_the\\_Ukrainian\\_State\\_and\\_Defence\\_Forces/](https://www.researchgate.net/publication/314755402_Russian_Information_Campaign_against_the_Ukrainian_State_and_Defence_Forces/)

<sup>8</sup> Kania, Elsa B, and John K Costello. "The Strategic Support Force and the Future of Chinese Information Operations ." US Army Cyber Defence Review, 2018. Accessed on 10<sup>th</sup> April 2021 [https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force\\_Kania\\_Costello.pdf](https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf).

<sup>9</sup> Fravel, Taylor M. "China's New Military Strategy: 'Winning Informationised Local Wars.'" The Jamestown Foundation, July 2, 2015. Accessed on 10<sup>th</sup> April 2021 <https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/>.

<sup>10</sup> N.5

<sup>11</sup> N.2



<sup>12</sup> Cook, Chaveso, and Liam Collins. "PSYOP, Cyber, and InfoWar: Combating the New Age IED." Modern War Institute, April 6, 2021. Accessed on 09<sup>th</sup> April 2021 <https://mwi.usma.edu/psyop-cyber-and-infowar-combating-the-new-age-ied/>.

<sup>13</sup> Shishir Gupta, Rezaul H Laskar, and Yashwant Raj. "India, Pakistan Came Close to Firing Missiles at Each Other on February 27." Hindustan Times, March 23, 2019 Accessed on 19 March 2021. <https://www.hindustantimes.com/india-news/india-pakistan-came-close-to-firing-missiles-at-each-other-on-february-27/story-rVsBjZ5qmxXMprktzDNqcM.html>.

<sup>14</sup> M.K., Nidheesh. "Abhinandan a Picture of Courage, Calm amid India-Pakistan Conflict." The Live Mint, February 28, 2019. Accessed on 19 March 2021 <https://www.livemint.com/news/india/abhinandan-a-picture-of-courage-calmness-amid-growing-india-pakistan-conflict-1551318333696.html>.

<sup>15</sup> Divya Malhotra, 'Inter-Services Public Relations (ISPR): Assessment of the Pakistan Military's Discreet Propaganda Factory Post-1990', *Manohar Parrikar Institute for Defence Studies and Analyses*, Journal of Defence Studies, Vol. 14, No. 4, October–December 2020, pp. 37–57, n.d., 22.

<sup>16</sup> Xin Liu, Guoyuandan, and Zhang Hui, 'China Unveils Details of 4 PLA Martyrs at Galwan Valley Border Clash for First Time, Reaffirming Responsibility Falls on India - Global Times', accessed 13 June 2021, <https://www.globaltimes.cn/page/202102/1215914.shtml>.

<sup>17</sup> Ananth Krishnan, 'China's Media Puts out What Seems to Be Another New Video from the Galwan Valley Clash of June 2020 (from the Mentioned Weibo Account) <https://t.co/T3jiGDBfeE>', Twitter, @ananthkrishnan (blog), 22 February 2021, <https://twitter.com/ananthkrishnan/status/1363678480190218243>.

<sup>18</sup> Abhijit Singh, 'China's "Three Warfares" and India', *Institute for Defence Studies and Analyses*, Journal of Defence Studies, 7, no. October December (n.d.): 22–46.

<sup>19</sup> Ibid

<sup>20</sup> Balram, Smita. "Covid-19 Impact: Social Media Activity in the Country Grew 50X in Early March, Says Nielsen." The Economic Times, March 28, 2020 (Accessed on 03 April 2021 ). <https://economictimes.indiatimes.com/tech/internet/covid-19-impact-social-media-activity-in-the-country-grew-50x-in-early-march-says-nielsen/articleshow/74833596.cms?from=mdr>.

<sup>21</sup> Ortiz-Ospina, Esteban. "The Rise of Social Media." Our World In Data, September 18, 2018. Accessed on 19 March 2021 <https://ourworldindata.org/rise-of-social-media>. Accessed

<sup>22</sup> Tankovska, H. "Facebook Users by Country 2020." Statista, February 9, 2021. Accessed on 19 March 2021 <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>.

<sup>23</sup> "Digital India." Common Services Centres Scheme. Accessed April 2, 2021. <https://csc.gov.in/digitalIndia>.

<sup>24</sup> IANS. "Over 500 Million Indians Now Use SMARTPHONES, Report Claims." Gadgets360. NDTV, January 30, 2020. Accessed on 03 April 2021 <https://gadgets.ndtv.com/mobiles/news/over-500-million-indians-now-use-smartphones-77-percent-of-who-are-online-techarc-2172219>.



- <sup>25</sup> Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health--and How We Must Adapt*, 2020, Currency Press. PP- 97
- <sup>26</sup> Lauren E Sherman et al., 'What the Brain "Likes": Neural Correlates of Providing Feedback on Social Media', *Social Cognitive and Affective Neuroscience* 13, no. 7 (4 September 2018): 699–707, <https://doi.org/10.1093/scan/nsy051>.
- <sup>27</sup> 'The Psychology of Social Media', King University Online, 19 September 2019, Accessed June 26 2021 <https://online.king.edu/news/psychology-of-social-media/>.
- <sup>28</sup> N.24 & Mike Allen, 'Sean Parker Unloads on Facebook: "God Only Knows What It's Doing to Our Children's Brains"', Axios, November 09 2017 accessed 27 June 2021, <https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html>.
- <sup>29</sup> 'Media Tweets by Jay Wankhade (@jaywankhadejr) / Twitter', May 24<sup>th</sup> 2021 , accessed 27 June 2021, <https://twitter.com/jaywankhadejr/status/1396871561001390083>. (Note: The original source of this image remains to be ascertained)
- <sup>30</sup> 'Special Forces of India', February 19 2021, accessed 27 June 2021, <https://www.facebook.com/specialforceofindia/photos/a.1465345287018566/2958470841039329/?type=3&theater>. (Note: The original source of this image remains to be ascertained)
- <sup>31</sup> Ebstein, R. P., Novick, O., Umansky, R., Priel, B., Osher, Y., Blaine, D., et al. "Dopamine D4 receptor (D4DR) exon III polymorphism associated with the human personality trait of Novelty seeking", 1996, *Nature Genetics*, 12(1), 78–80.
- <sup>32</sup> 'Army Is Worried about Social Media Usage by Its Soldiers; Here's Why', July 10 2019, accessed 29 June 2021, <https://www.timesnownews.com/mirror-now/in-focus/article/army-is-worried-about-social-media-usage-by-its-soldiers-heres-why/451129>.
- <sup>33</sup> Crone, Eveline A, and Elly A Konijn. "Media use and brain development during adolescence." *Nature communications* vol. 9,1 588. 21 February 2018, accessed June 26 2021 doi:10.1038/s41467-018-03126-x.
- <sup>34</sup> Wenger, Jennie W., Heather Krull, Elizabeth Bodine-Baron, Eric V. Larson, Joshua Mendelsohn, Tepring Piquado, and Christine Anne Vaughan, *Social Media and the Army: Implications for Outreach and Recruiting*. Santa Monica, CA: RAND Corporation, 2019. Accessed 02 July 2021 [https://www.rand.org/pubs/research\\_reports/RR2686.html](https://www.rand.org/pubs/research_reports/RR2686.html).
- <sup>35</sup> 'How Are Social Media Sites Changing China?', *BBC News*, 1 September 2012, accessed 3 July 2021, <https://www.bbc.com/news/av/world-asia-china-19399773>.
- <sup>36</sup> 'Exploring Chinese Military Thinking on Social Media Manipulation Against Taiwan', Jamestown, 12 April 2021, accessed 3 July 2021, <https://jamestown.org/program/exploring-chinese-military-thinking-on-social-media-manipulation-against-taiwan/>.
- <sup>37</sup> Eva-Karin Olsson, Edward Deverell, Charlotte Wagnsson & Maria Hellman (2016): EU armed forces and social media: convergence or divergence?, *Defence Studies*, DOI: 10.1080/14702436.2016.1155412



- <sup>38</sup> Johnson, Amy, Celeste Lawson, and Kate Ames. "'Use Your Common Sense, Don't Be an Idiot': Social Media Security Attitudes amongst Partners of Australian Defence Force Personnel." *Security Challenges* 14, no. 1 (2018): 53-64. Accessed July 3, 2021. <https://www.jstor.org/stable/26488491>.
- <sup>39</sup> Lieutenant Colonel E.J.G. Groulx, 'Use of Social Media in the Canadian Armed Forces Primary Reserves - Facebook - "Friend" or Foe?', n.d., 64.11 January 2015, Accessed 03 July 2021, <https://www.cfc.forces.gc.ca/259/290/296/286/groulx.pdf>
- <sup>40</sup> 'Russia Bans Smartphones for Soldiers over Social Media Fears', BBC News, 20 February 2019 sec. Europe, Accessed 03 July 2021 <https://www.bbc.com/news/world-europe-47302938>.
- <sup>41</sup> Dev Ankur Wadhawan 'Rajasthan: Honey-Trapped Army Jawan Arrested on Charges of Spying, Leaking Confidential Info to Pakistan', India Today, March 15 2021 accessed 28 June 2021, <https://www.indiatoday.in/india/story/rajasthan-honey-trapped-army-jawan-arrested-on-charges-of-spying-leaking-confidential-info-to-pakistan-1779323-2021-03-15>.
- <sup>42</sup> Government of India, The Army Act 1950, May 20, 1950, Clause 21, <https://www.mod.gov.in/sites/default/files/TheArmyAct1950.pdf>, Accessed 19<sup>th</sup> September 2021
- <sup>43</sup> 'Punjab: Army Jawan Was at Farmers' Protest | Chandigarh News - Times of India', The Times of India, January 6 2021 accessed 29 June 2021, <https://timesofindia.indiatimes.com/city/chandigarh/agencies-identify-army-jawan-who-took-part-in-stir-in-military-uniform/articleshow/80125253.cms>.
- <sup>44</sup> 'Nearly 1 In 5 Defendants In Capitol Riot Cases Served In The Military', NPR.org, January 21 2021 accessed 29 June 2021, <https://www.npr.org/2021/01/21/958915267/nearly-one-in-five-defendants-in-capitol-riot-cases-served-in-the-military>.
- <sup>45</sup> 'BSF Jawan Video: Govt Takes "Serious Note", Says Welfare of Soldiers a Priority', Hindustan Times, 10 January 2017, Accessed June 29 2021 <https://www.hindustantimes.com/india-news/bsf-jawan-video-govt-takes-serious-note-says-welfare-of-soldiers-a-priority/story-7cg0iv7TVm98omfoVpLyjN.html>.
- <sup>46</sup> Excerpts from an interview with a serving officer in Indian Army
- <sup>47</sup> What the author means by social isolation is the soldier being away from his family and friends. When the soldier is on duty his relationships with other service members are being considered as professional relationships.
- <sup>48</sup> 'Nearly 80 Percent of Social Media Time Now Spent on Mobile Devices', MarTech, 4 April 2016, Accessed June 29 2021, <https://martech.org/facebook-usage-accounts-1-5-minutes-spent-mobile/>.
- <sup>49</sup> Kuss, Daria J., and Mark D. Griffiths 2017. "Social Networking Sites and Addiction: Ten Lessons Learned" *International Journal of Environmental Research and Public Health* 14, no. 3: 311. <https://doi.org/10.3390/ijerph14030311>
- <sup>50</sup> Neal, Stephenson 'A Quote from Snow Crash', accessed 3 July 2021, <https://www.goodreads.com/quotes/359739-see-the-world-is-full-of-things-more-powerful-than>.
- <sup>51</sup> '77th Brigade', accessed 1 July 2021, <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/>.





---

<sup>52</sup> Sir David Omand, Jamie Bartlett & Carl Miller (2012) Introducing Social Media Intelligence (SOCMINT), Intelligence and National Security, 27:6, 801-823, DOI: 10.1080/02684527.2012.716965

<sup>53</sup> U.S Office of the Chairman of the Joint Chiefs of Staff., Joint Publication 3-0: Joint Operations, January 17, 2017, Accessed June 03 2021, III-15, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_0ch1.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf)

<sup>54</sup> 'Manhunting the Manhunters: Digital Signature Management in the Age of Great Power Competition', Modern War Institute, 3 May 2021, Accessed 29 June 2021, <https://mwi.usma.edu/manhunting-the-manhunters-digital-signature-management-in-the-age-of-great-power-competition/>.

---

*The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.*



**CENTRE FOR LAND WARFARE STUDIES (CLAWS)**

RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010

Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: [landwarfare@gmail.com](mailto:landwarfare@gmail.com)

Website: [www.claws.in](http://www.claws.in)