ASA Research Note

# Social Media and Information Warfare: The New Warfront

**Author:** Tiffany Pham

**Published:** November 2022

**Written:** March 2022

**Keywords:** Social media; information warfare; disinformation; international conflict

**Abstract:** The paper discusses the evolution of social media platforms and content from information-sharing spaces to a communication medium that is being used both as a propaganda tool and a tactical weapon during conflicts. Social media has created a new warfront in geopolitical conflicts where opposing sides engage in a form of combat with consequences that are both physical and destructive. The weaponization of social media has presented itself in multiple ways, and can have far-reaching impacts during almost any type of conflict.

---

American citizens in the Vietnam war era first witnessed–via journalism and televised news–the realities of war, much to their horror. But in the context of modern warfare, social media now competes with these "filtered" mediums. Rather than being used *solely* to relay news and updates and "realities," social media has become an information weapon that is just as influential as infantry on the ground, presenting the world with new ways to spread propaganda, new tactically offensive uses, and new ways to share humanitarian developments. Altogether they form a new warfront on which all nations must now engage in warfare – a new space where opposing entities engage in combat.

While propaganda is not a new phenomenon, the advent of social media has crafted a new medium that allows its intended message to reach a far wider audience and with greater ease. The use cases of social media as a propaganda tool can be further divided into several categories to reflect the purposes of its engagement in military operations or during times of war. While most of those categories align to the traditional World War-esque notions and purposes of propaganda, social media allows two tactics to be executed well in comparison to its pre-technology predecessors. The first type, misinformation or disinformation, has perhaps become well known as of the United State's contentious 2016 election, but presents itself differently in the context of war. Pro-Russian disinformation, amid the ongoing Ukrainian-Russian war, demonstrates that disinformation in times of an election appear to be with the purpose of attaining a specific outcome, such as electing a desired candidate, whereas disinformation in times of war appear to justify or sustain military operations and active

conflicts. Recently, Meta, formerly Facebook, "separately removed a network of about 40 fake accounts, groups and pages across Facebook and Instagram that operated from Russia and Ukraine targeting people in Ukraine…" [1] by launching cyberattacks *and* posting alleged videos of Ukrainian soldiers surrendering with a white flag, along with claims that Ukraine is a "failed" or unlawful state: all deemed "coordinated inauthentic behavior" by Meta. While an argument can be made for several intended purposes, this type of disinformation overall attempts to sustain a military conflict by raising the morale of those already in favor of conflict (the surrender video), and justifies the war to the skeptics (the claims of Ukraine being a failed or illegitimate or "Nazified" state). Its spread on social media, however, allows it to reach an audience in *allied* nations such as India, where Russia has enjoyed historically friendly relations and "tacit support" for the ongoing conflict.[2] It should be noted that the intention of this research is not to create political implications, and in fact there are several *verifiable* reasons that many Indian citizens support Russia, but the intention is to observe the similarity in language from Russia disinformation channels to growing popular opinion from certain Indians online. Twitter user Tarun Raju, featured in a Quartz overview of how Indians on the internet view the situation uses near identical phrasing as known disinformation channels when he writes:

> "Do NOT trust the Ukrainians. Ukraine is now stateless, and run by neo-Nazi warlords. Ukrainian political leadership is probably tucked in safe behind NATO lines. The Ukrainian govt is only involved in active hostilities with Russia, it's not running the country..."[3]

In another one of his tweets featured by Quartz, with a sizable 1,155 retweets and 2,871 likes, he refers to the current Ukrainian government as the Maidan Regime, echoing Russian sentiment that the government that took power in the aftermath of the Euromaidan protests is illegitimate and corrupt.[4] This demonstrates the use of social media as a platform for disinformation in that Russia has created a transmittable, unified narrative far beyond the reaches of a single target audience, allowing a conflict to be vocally sustained and justified by more than just the initial aggressors. In the context of war, it is akin to gaining more soldiers on the online front.

In addition, social media can be used to divert attention and desensitize civilian populations. Disinformation is not a required component though it is commonly used. In this example, TikTok, with its trademark premise of short, fun, digestible video clips, demonstrates the usage of social media as a desensitization and diversion tool uniquely. To start, the Israel Defense Forces–Israel's official combined military–boasts its *own* official TikTok page on which conventionally attractive young female soldiers perform popular dances and handsome male soldiers post meme videos; all in uniform, and all against the backdrop of Israeli airstrikes

 

against Gaza, in which 240 civilians were killed.[5] One particular Israeli figure, Natalia Fadeev, is a reservist in the IDF and a member of the Alpha Gun Angels, a "gun-modeling and social media–marketing agency, (made up of) a team of nine active and veteran IDF combat soldiers turned Instagram celebrities." Their clients include the IDF.[6] In her own offshoot TikTok account she posts dances, lip syncs to trending songs, and poses with weaponry. One video with 326,000 likes boasts the caption: "stop spreading lies about Israel IL we have the most moral military!" with the video itself featuring snapshot like poses from Fadeev, text running across the screen that says "I proudly served as a Military Police Officier [*sic*] in the IDF now tell me, do I look like I could harm innocent civilians?"[7] Israel's appeal to the younger, more tech-savvy generation who frequents TikTok does not begin there. P.W. Singer, a consultant for the U.S. military explains that Israel had previously created an online army for students, not limited to Israel itself, to "join the online battle" via apps that ask users to retweet Israeli narratives in an attempt to influence military targets, earning the player promotions and badges for their "service," essentially having gamified its military operations.[8]

While some may find Israel's usage of TikTok to spread the glamorized image of a fun, military career and bolster recruitment fairly blatant–straight out of satirical news, sans the irony–the IDF somehow still accomplishes its military goal quite well: that of diversion and desensitization. One need only refer to its comment section. And yet even if many were to have the opinion that Israel's heavy-handed attempt to appeal to the youth is too obvious to be effective, it is a spectacle that turns eyes all the same. The civilian perception of its military as professional and efficient is one image worth fostering, but a harmless, clownish image–from the point of view of the amused but "immune to propaganda" crowd–or a fun, unified image–from the point of view of truly convinced youths–are both more "fun" and subversive, as most already expect a country's military to be professional. An important note is that according to Statista Research, "37.3 million of (TikTok) users belonged to Generation Z'' [9] meaning they–the largest demographic on TikTok–are ages 10-19: Israel's target audience. With social media, less research is required when selecting targets as compared to past conflicts, where demographics, beliefs, and geographic location had to be studied and accounted for in sophisticated, crafted propaganda campaigns. Rand Waltzman, in his 2017 testimony on The Weaponization of Social Media states that the first four steps of a typical offensive campaign are as follows;

1. Take the population and break it down into communities, based on any number of criteria (e.g. hobbies, interests, politics, needs, concerns, etc.).
2. Determine who in each community is most susceptible to given types of messages.
3. Determine the social dynamics of communication and flow of ideas within each community.
4. Determine what narratives of different types dominate the conversation in each community.[10]

Now, social media simply with its known demographics and its subgroups clearly labeled with a community's beliefs–such as a Facebook page for an alt-right group– allows a nation at war to select a platform and simply send its message at a unprecedented speed, helping it to achieve goals such as further enlistments in its armed forces.

Another emerging use for social media in times of war is as a tactical weapon, characterized by an initial phase of information gathering or espionage and paired with social engineering to execute military deception strategies. Whereas social media as a vehicle for platform targets the civilian population, this category is strictly related to direct interactions with military units and active combatants to gain a strategic advantage. The first stage of social media as a tactical weapon is often its usage as a vehicle for espionage and information gathering. This first phase of intelligence gathering naturally informs tactical decisions, or offensive moves, and it is made easier by the volume of public information available on social media. The casual context in which most users use Facebook or Instagram for example, makes it unlikely for an enemy to approach a specific rank-and-file individual for information or with hostile intent. In fact, the premise of social media–to share moments, connect with others, and talk or exchange information–may psychologically prime its audience for neutral to positive interactions when specifically approached by *one* other individual (and it is likely very different if engagement consisted of passive consumption of multiple peoples' content). This concept was shown in 2017, when NATO's Strategic Communications Center of Excellence engaged in online espionage as part of a mock offensive operation in order to test the security of a military whose origin nation is classified. The red team utilized open source intelligence analysis, impersonation, honeypot pages (fake Facebook pages designed to lure soldiers into joining) and finally *individual* social engineering, once contact could be established with the select soldiers who fell for the trap. As a result of this exercise, the red team was able to "identify all members of certain units, pinpoint the exact locations of several battalions, gain knowledge of troop movements to and from exercises, and discover the dates of the active phases of the exercise," with locations being accurate within plus or minus one kilometer.[11] This is a simulated attack, meaning that the role of an information seeking enemy is played out by an ethical, allied entity whose purpose is ultimately to identify risks and improve security. The concept of social media espionage and intelligence gathering in *unsimulated* warfare briefly became realized during the Ukrainian-Russian War, when Russian soldiers recklessly utilizing their Tinder accounts–with its location-based matching services–began appearing in the feeds of nearby Ukrainian women. Due to the sheer volume of Russian soldiers appearing in the suggested pool of nearby Ukrainian Tinder users, the Ukrainian military was then able to infer the location of Russian forces.[12]

Valuable information such as troop movements or locations are of course the pieces that then inform tactical decisions. Just like its preceding intelligence gathering actions, these tactical maneuvers (strategies that directly impact the conflict on the ground) are also being executed with social media. The term "the weaponization of social media"' or "social media as an information weapon" become most literal within this category. An early example can be found by in ISIS' invasion of Iraq, in which ISIS with their "legions of fans and botnets on Twitter…coalesced around a hashtag, #AllEyesOnISIS," essentially broadcasting their invasion and generating fear in 30,000 Iraqi soldiers, who began to retreat and abandon equipment in the belief that ISIS was already well-prepared and advancing, when in reality ISIS had 1,500 fighters.[13] Non-governmental humanitarian aid organization Mercy Corp describes a later example of social media used to gain a tactical advantage within Russia's online defamation campaign of the Syrian White Helmets, a Syrian humanitarian organization painted as a terrorist organization by Russian botnets, which led to an increase in attacks on the White Helmets and decreased operations.[14] Both situations allowed the aggressor to gain a military advantage, and while military deception, psychological operations, and information war are not new topics in warfare, social media as a tactical weapon does one thing much more efficiently than traditional military deception: amplification, which the Mercy Corp defines (in the context of social media) as narratives made prominent "via botnets, inauthentic accounts, influencers, hashtag hijacking, astroturfing(imitating grass-roots actions using coordinated inauthentic accounts) and trading up the chain (planting stories in small outlets where they can then be picked up by larger ones)"[15] Gone are the days of erecting inflatable "jets" and military equipment to deceive the enemy on one's capabilities, when starting a trending topic on Twitter does much the same.

Finally, perhaps the most recent and emotionally moving development is the use of social media to facilitate or appeal to humanitarian purposes. This may include documenting war crimes via images or videos spread on social media depicting civilian deaths or corpses, even that of children. One of the affordances of social media *is* the ability to share pictures and videos in color, real-time, and without the filter of professional commentary. Thus, the use of social media for humanitarian purposes sets itself apart from televised news, where verbal commentary is present and gory content is blurred out. People now have the grim ability to see people being killed and other universally moving events as it happens, with graphic detail. Such pathos-building images influence warfare both by impacting popular support for all parties involved, the soldiers, government, and civilians alike. Once more turning to the Ukrainian-Russian war where this category is being demonstrated, one can turn to the establishment of social media pages (notably Twitter and Telegram, though a hosted website is also present) by representatives of the Ukrainian interior ministry, with the purpose of body-identification and

 

information for Russian families whose loved ones had been sent to war and whose status is unknown. The website known as 200rf.com and the Twitter handle known as @rf200_now (both of which reference the phrase Cargo 200, for the cargo that transports the dead bodies of fallen soldiers) feature graphic images of deceased soldiers for Russians to search for their family members among the dead.[16] Social media documenting humanitarian developments, such as dead soldiers left by their home nation or fleeing refugees, now impacts warfare in terms of morale and popular support on an international level. It establishes images of one country's behavior as opposed to the other–through grainy pictures and phone-captured videos of fallen Russian soldiers being left behind by their own, for example, in contrast to Ukrainian humanitarian-based social media such as rf200_now–*along* with one country's impact on the other, and more. As wars continue to be waged, this particular use case of social media will continue to grow.

In a war of chaos and disarray, it often falls to social media giants such as Meta and Twitter to regulate as events unfold and play defense in the battle, as they most recently did in the example of disinformation during the Ukrainian-Russian war. However, one recommended, all-encompassing defense mechanism to combat social media as an information weapon–be it against propaganda or tactical usage in particular–is to proactively dedicate a government sector to information security. This is a tried and tested method already within the Czech Republic, which boasts an established Center Against Terrorism and Hybrid Threats (CTHT) and the Czech Security Information Service (*Bezpečnostní informační služba*) that proactively, and with access to classified information, is dedicated to "reviewing disinformation, preparing policy proposals, and working with other government agencies and outside organizations to raise awareness…(and) to resist intrusions…planning for election-related attacks and mitigating vulnerabilities" with a focus on Russian methods in particular. And as lauded by the Center for Strategic & International Studies, these organizations continue to operate effectively even when current government leaders are *explicitly* pro-Russian themselves.[17] The American approach in comparison is to–in line with free-market beliefs–allow the private corporations to act as an individual and protect its own platform, with the nation's security benefiting as a byproduct. In contrast, the proposed defense is to 1) put defensive recommendations and requirements in the hands of a third party organization, preferably attached to the Department of Defense and 2 ) be proactive. Meta for example, must address hacking attempts and remove bot accounts as they are happening or discovered, with varying degrees of success and high profile failures. Only after these trials are the lessons learned translated into formal terms and conditions for future use. Even with terms and conditions in place, however, the research team from the aforementioned NATO StratCom penetration test found that several illegitimate accounts and pages either took 2 weeks to be suspended by Facebook or were simply *never*

 

removed at all.[18] One final recommendation is to supplement a specialized government department with an updated cyber kill chain adapted specifically to social media campaigns to standardize the language around the weaponization of social media and its processes, in order to provide a "cognitive mental model" as described by the Journal of Information Warfare by Peregrine Technical Solutions.[19]

In the minds of many, every nation and its people have perhaps already been tarnished by the weaponization of social media. Its impact has led to further international division, disillusionment, and distrust, and in that way many are already victims of online warfare by virtue of being online, caught in the crossfire of a tweet, or a targeted video on YouTube. However, in the context of an active war, the consequences are physical and destructive. The online aspect is thus part of the battle. Social media, whether utilized as a propaganda tool or as a tactical weapon, has solidified this new front of war. More likely than not, it will remain a permanent one.

## SOURCES


[1] Elizabeth Culliford, "Facebook-Owner Meta Says Ukraine's Military, Politicians Targeted in Hacking Campaign," Reuters (Thomson Reuters, February 28, 2022), https://www.reuters.com/technology/facebook-owner-meta-says-ukraines-military-politicians-targeted-hacking-campaign-2022-02-28/.

[2] Umang Poddar, "How Indians on the Internet View India's Tacit Support of Russia," Quartz (Quartz, March 1, 2022), https://qz.com/india/2136155/how-indians-on-the-internet-view-indias-tacit-support-of-russia/.

[3] Raju, Tarun (@btarunr). "Do NOT trust the Ukrainians. Ukraine is now stateless, and run by neo-Nazi warlords. Ukrainian political leadership is probably tucked in safe behind NATO line." Twitter, February 25, 2022, 8:22 PM. https://twitter.com/btarunr/status/1497426768831348739?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497426768831348739%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcms.qz.com%2Fembed-sandbox%2F2136155%2Ftwitter.com%2Fbtarunr%2Fstatus%2F1497426768831348739

[4] IBID, p.2

[5] EJ Dickson, "Why Are Israeli Defense Forces Soldiers Posting Thirst Traps on TikTok?," Rolling Stone (Rolling Stone, May 28, 2021), https://www.rollingstone.com/culture/culture-features/israel-defense-force-idf-tiktok-thirst-trap-1174211/.

[6] Sophia Goodfriend, "Naked Gun," Jewish Currents, December 5, 2019, https://jewishcurrents.org/naked-gun/.

[7] Fadeev, Natalia. @Gun Waifu, "IDF Military Police reservist IL Airsoft player • ALL LINKS ON IG •", TikTok, March 8, 2022 https://www.tiktok.com

[8] Dave Davies, "The 'Weaponization' of Social Media - and Its Real-World Consequences," NPR (NPR, October 9, 2018), https://www.npr.org/2018/10/09/655824435/the-weaponization-of-social-media-and-its-real-world-consequences.

[9] U.S. TikTok Users by Age 2021," Statista, January 28, 2022, https://www.statista.com/statistics/1095186/tiktok-us-users-age/.

[10] *The Weaponization of Information, The Need for Cognitive Security*, Senate Armed Services Committee, Subcommittee on Cybersecurity (statement of Rand Waltzman, RAND Corporation) April 17, 2017.

[11] Bay S., Bertolin G., Biteniece N., Christie E., Dek A., Fredheim R., Gallacher J.D., Kononova K., Marchenko T.,. Responding to Cognitive Security Challenges. Riga: NATO Strategic Communications Centre of Excellence. February 12, 2019 https://stratcomcoe.org/publications/responding-to-cognitive-security-challenges/113

[12] Nick Parker, "Russian Soldiers Are Chasing Ukrainian Girls," news.com.au, The US Sun, February 25, 2022, https://www.news.com.au/lifestyle/relationships/dating/russian-soldiers-are-chasing-ukrainian-girls-on-tinder/news-story/d730ab5a9cb90702365c06973b577ad7.

[13] IBID, p.4

[14] The Weaponization of Social Media: How Social Media Can Spark Violence and What Can Be Done about It," The Mercy Corps, November 2019, https://ap9.mercycorps.org/sites/default/files/2020-01/Weaponization_Social_Media_FINAL_Nov2019.pdf.

[15] IBID, p.7

[16] Helene Cooper and Eric Schmitt, "Russian Troop Deaths Expose a Potential Weakness of Putin's Strategy," The New York Times (The New York Times, March 1, 2022), https://www.nytimes.com/2022/03/01/us/politics/russia-ukraine-war-deaths.html.

[17] "Countering Russian Disinformation," Center for Strategic and International Studies, September 25, 2020, https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation.

[18] IBID, p.6

[19] Bergh, A. "Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach." *Journal of Information Warfare* 19, no. 4 (2020): 110–31. https://www.jstor.org/stable/27033648.