Hadtudományi Szemle
18. évfolyam (2025) 2. szám 91–106. • DOI: 10.32563/HSZ.2025.2.6

Barbara Fábri[1]

The War That Went Viral

The Russian–Ukrainian War on Social Media

Abstract

This study explores the role of social media – particularly Twitter, Reddit, and TikTok – in modern warfare, using the Russian–Ukrainian war as a case study. It identifies six key areas where social media functions as a tool of warfare: intelligence gathering, target acquisition, information operations, cyberspace activities, defence strategies, and command and control. The research employs a qualitative approach to analyse how these platforms shape public perception, facilitate cyberattacks, and assist in strategic coordination while also addressing challenges such as misinformation, bias, and ethical concerns. By building on hybrid warfare and information operations theories, the study underscores how social media blurs the lines between traditional media and the battlefield. Ultimately, it calls for interdisciplinary methodologies to better understand the strategic impact of social media in contemporary conflicts.

Keywords: social media, information operations, hybrid warfare

Introduction

The role of social media in modern warfare has fundamentally altered the dynamics of conflict, particularly within the context of the Russian–Ukrainian war. This paper explores how social media platforms, notably Twitter, Reddit, and TikTok, serve as essential tools in hybrid warfare and information operations, blurring the lines between traditional media and the battlefield. These platforms enable intelligence gathering, influence public perception, and coordinate both offensive and defensive actions.

The article highlights six key areas where social media serves as a tool of warfare: intelligence and reconnaissance, target acquisition, information and influence, cyberspace operations, defence, and command and control. Through real-life cases

[1] PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: b.bihaly@gmail.com

from the Ukrainian crisis, it demonstrates how social media facilitates intelligence gathering, target identification, narrative shaping, cyberattacks, operational security, and coordination of actions.

The article explores how the Ukrainian crisis has affected the use of social media in warfare, emphasising the importance of platforms like Twitter, Reddit, and TikTok in spreading information, moulding narratives, and swaying public perception. It also addresses the challenges associated with collecting and analysing social media data for research, including issues related to bias, misinformation, and geolocation restrictions.

The essay's conclusion highlights how social media has transformed modern warfare, erasing distinctions between traditional media and the battlefield. It acknowledges the complexities of using social media as a tool of war and promotes a nuanced comprehension and interdisciplinary methods for analysing its impact on present-day conflicts.

Building upon this foundation, the research constructs a robust conceptual framework elucidating the nuances of the integration of social media into warfare strategies. It delineates key concepts including hybrid warfare, information operations, and the strategic deployment of social media for intelligence gathering, influence, and cyber operations.

The research conducts a qualitative analysis of the amassed data, employing rigorous methodologies to decipher underlying patterns, trends, and narratives. Through this analytical lens, the essay unveils the intricate interplay between social media dynamics and the evolving landscape of modern warfare.

Throughout the analysis, the research adopts a critical perspective, contemplating the intrinsic limitations and obstacles associated with employing social media as a research instrument in conflict regions. It wrestles with concerns regarding bias, misinformation, and ethical dilemmas, emphasising the importance of careful evaluation and scrutiny when interpreting data from social media sources.

Hypotheses

1. Social media platforms have become potent instruments in contemporary warfare, blurring the lines between traditional media and the battlefield.
2. The social media has been transformed in the modern conflict area, particularly in the context of the Ukrainian crisis, by illustrating how it facilitates intelligence gathering, target identification, narrative shaping, cyber operations, operational security, and coordination of actions.

Methodology and data collection

To substantiate the paper's claims, a more detailed explanation of data collection methods is essential. A qualitative analysis of social media data was conducted, drawing from OSINT tools, geotagged posts, and sentiment analysis algorithms.

Ethical considerations, such as ensuring data authenticity and minimising bias, were carefully integrated into the research framework.

However, challenges remain in terms of data verification. Social media content is notoriously difficult to authenticate, and bot activity or deliberate state-led disinformation campaigns can compromise the integrity of open-source data. Further research should explore how to develop more robust methods of fact-checking and verifying content during ongoing conflicts.

Introduction: social media in the hybrid war

Research into social media's role in conflict zones has gained momentum, with scholars such as Thomas Elkjer Nissen[2] and Sanda Svetoka[3] providing foundational insights into how platforms like Facebook and Twitter influence information warfare. However, recent studies on Reddit and TikTok, two platforms with significant growth in user-generated content during the Russian–Ukrainian conflict, remain underexplored.

Moreover, while there is significant research into the role of social media in Western military operations, there is a comparative lack of focus on non-Western perspectives, especially regarding how platforms like Weibo or VKontakte may play similar roles in Eastern European conflicts.

Information used as an element of warfare and national power is as old as civilisation itself; however, the emergence of the information age ensured the exponential

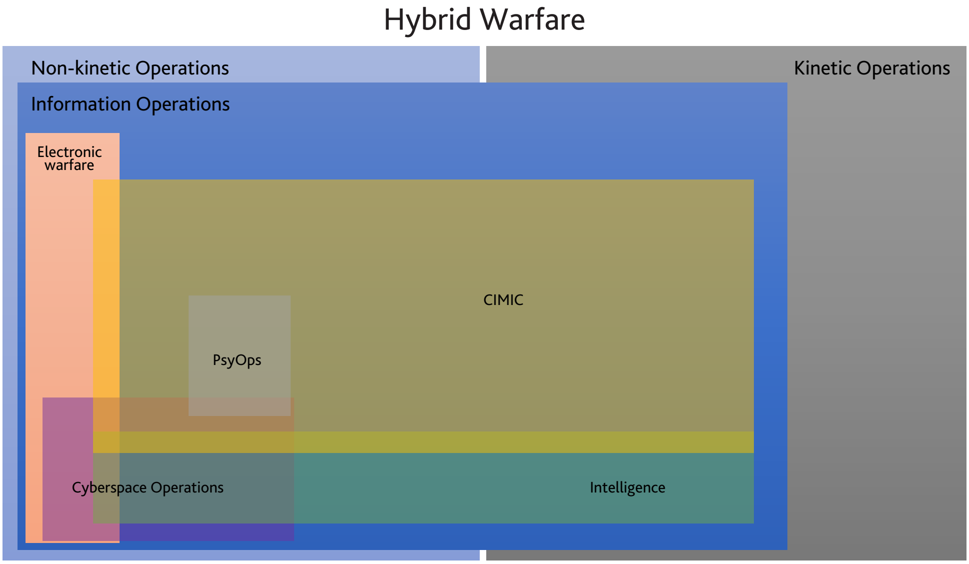

Figure 1: Hybrid operations
Source: compiled by the author

[2] Nissen 2015.

[3] Svetoka 2016.

proliferation of tactics, technologies, and threats to relate to the simple new art and science of information operations (IO). The emergence of Web 2.0 technologies, especially social media, and their subsequent use for military purposes represents an evolution in military affairs that creates an opportunity to level the playing field between major and minor powers and non-state actors around the world.

Hybrid warfare, in a classical sense, means the use of kinetic and non-kinetic operations side by side, and sometimes they are overlapping each other. While kinetic operations take place in the physical (real) dimension, targeting infrastructures existing in the physical space, non-kinetic operations usually take place in the information space and cognitive dimension, first preceding kinetic operations, and later (ideally) supporting them in accordance. Also, there are impact based operations in the information domain, which means one launches an operation within the information domain, but the end state will have an effect in the physical dimension. As far as we know, the aim of hybrid operations was to keep the conflict below the war threshold, but this paradigm seems to be overturned with the current war in Ukraine.

Hybrid warfare combines conventional military force with irregular tactics, including the use of cyber and information operations to disrupt the enemy's capabilities without direct engagement. This involves both kinetic operations (physical warfare) and non-kinetic operations (psychological and cyber warfare). Social media is pivotal in the latter, providing a venue for intelligence gathering, psychological operations, and the dissemination of disinformation.

In military terms, information operations (IO) are the integrated employment of electronic warfare, psychological operations, military deception, and operations security. Social media fits into this framework by enabling open-source intelligence (OSINT), providing a low-cost, high-reach medium for strategic communication, and facilitating target audience analysis.

The US-issued JP 3-13 doctrine on information operations[4] divides the information battlefield into the following three interrelated dimensions:

- physical dimension
- informational dimension and
- cognitive dimension.

This information dimension includes electromagnetic space, which overlaps with cyberspace, where cyber operations take place. Intelligence, reconnaissance operations and civil-military cooperation (CIMIC) also take place in this dimension. In light of this, psychological operations (PSYOPS) within CIMIC and various intelligence and reconnaissance operations (e.g. OSINT) can take place in information, electromagnetic and cyberspace in addition to the kinetic space as well. SM platforms can cater to the operational and strategical needs during conflict.

The real goal of both PSYOPS and reconnaissance operations is to gain information superiority over the adversary. And while, according to the initial interpretations, the focal point of information operations is the acquisition and maintenance of superiority,

[4] JP3-13 2006.

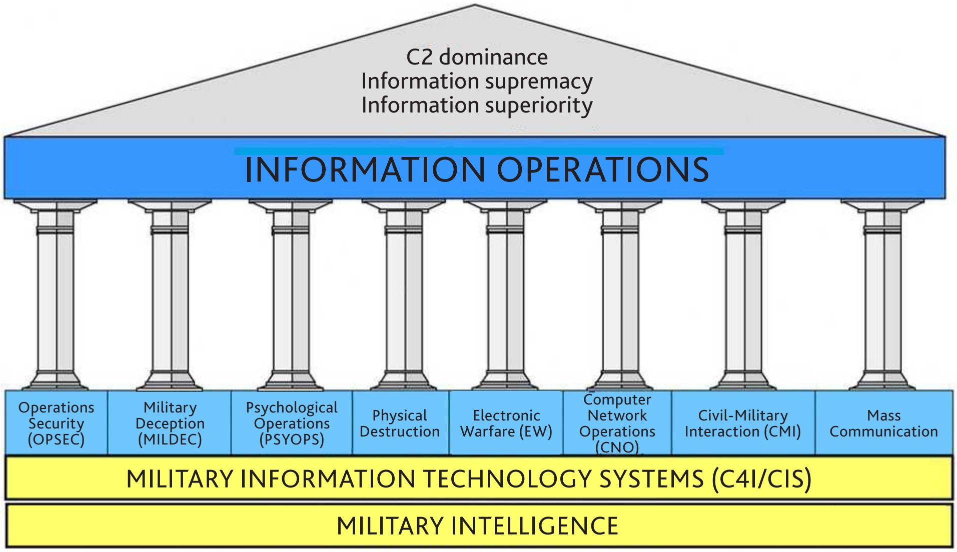
C2 dominance
Information supremacy
Information superiority
INFORMATION OPERATIONS
Operations Security (OPSEC)
Military Deception (MILDEC)
Psychological Operations (PSYOPS)
Physical Destruction
Electronic Warfare (EW)
Computer Network Operations (CNO)
Civil-Military Interaction (CMI)
Mass Communication
MILITARY INFORMATION TECHNOLOGY SYSTEMS (C4I/CIS)
MILITARY INTELLIGENCE

Figure 2: Information operations
Source: Haig 2018

nowadays during military operations, where the most affected layer in the information space is the civilian population, the goal is not for own forces to have more and better-quality information, or better ability to use it, but to win the target audience for the purposes of the military operation.[5]

Cyberspace (of which social media is increasingly a defining part) is often used during conflicts to knock out an adversary's communication systems. And cyberwarfare narratives tend to be limited to the computer systems that support our daily lives and businesses, maintain critical infrastructure, provide financial transactions, power, and more.[6]

Disruption or downtime of network and computer systems can have dramatic effects, but targeted narrative-driven operations can achieve results no less impressive than attacks on critical infrastructure.

Social media as a tool of warfare

We have already witnessed the use of social media in several international conflicts (Arab Spring, Syria, Ukraine) with the aim of conveying political and ideological goals, shaping public opinion, mobilising supporters, coordinating military activities (or successfully continuing strategic communication), as well as an undisclosed tool for collecting open information.

[5] Haig 2018.
[6] Svetoka 2016.

According to a study of Thomas Elkjer Nissen, social media support for military operations can be implemented in six areas: (1) intelligence, (2) target selection/identification, (3) information and influence (as in white and grey zone PSYOPS), (4) cyberspace operations, (5) defence, (6) C2 (command & control).[7] All these activities, regardless of whether they have online or offline effects, can be carried out through social media, mutually support each other, and can often be done in concert with kinetic activities.

1. *Intelligence and reconnaissance:* Focused search and analysis of information from social media networks and profiles, including content and conversations; these activities may be overt or covert. There are many approaches to social media information gathering analysis (e.g. trend, network, sentiment, geographic, content, behavioural, system, and information analysis). All of these forms of analysis can contribute to target audience analysis and support psychological warfare or target selection for online and offline operations. Basically, social media enables detailed information about networks, actors and related communications, helping any group to better understand the information environment and the situation of any target group without physical presence. When studied consistently, social media can be a useful source of situational awareness and even early warning signs of a future crisis.[8]
2. *Target acquisition:* social media can be used to identify potential targets for military action in kinetic space (based on geotagged images or social media conversations). For example, in Libya, Google Maps and cell phones were used to map regime positions, which were then transmitted to NATO, which used the information to identify targets.[9]
3. *Information and influence:* Nissen here refers to the dissemination of information to influence the values, belief systems, perceptions, emotions, motivation, reasoning and behaviour of the target audience.[10] The use of social media in this case seeks to achieve certain military effects in the cognitive space: it shapes, informs, influences, manipulates, exposes, reduces, promotes, deceives, forces, deters, mobilises, persuades.
4. *Cyberspace operations:* Targeting social media platforms and accounts, hacking password-protected sites, changing the content of a profile, or rendering a website completely unusable. These actions may include activities such as Distributed Denial of Service (DDoS) attacks on websites, hacking accounts using brute force, accessing and revealing the contents of emails or mobile phones, changing the content of social media accounts, or breaking into databases to gather information. All such activities are aimed at preventing other actors from using social media platforms, at least temporarily, to communicate, coordinate actions, access information or spread propaganda.[11]

[7] Nissen 2015.

[8] Nissen 2015: 62–64.

[9] Castillo 2015.

[10] Svetoka 2016: 67.

[11] Svetoka 2016: 65–66.

5. *Defence:* Nissen refers to a form of operational security (OPSEC) conducted within the confines of social media platforms, pages, profiles, and accounts at a technical or systemic level. Defensive measures may involve the utilization of encryption, anti-tracking, and/or IP-masking software in conjunction with social media.[12]
6. *C2:* Social media serves as a platform for internal communication, information dissemination, and the coordination and synchronisation of actions. Its use for command and control (C2) purposes is particularly vital for non-state actors like insurgent groups, particularly in cases where these groups lack a formal structure or are dispersed across vast geographical areas. Social media can function as a communication tool and a method to organise their endeavours. Nonetheless, employing social media also exposes the activities of insurgent groups to intelligence services.[13]

Effects of the Ukrainian crisis

The publication aims to present the six methods of using social media listed by Nissen through real-life cases. According to him, when using social media in hybrid operations, it is not civilian individuals, but soldiers or experts conducting planned operations that place influential, deceptive messages in social media content to deliberately change the narrative. It also should be taken into consideration, however, that these examples are only illustrative tools and do not serve as evidence of any event, as the contents are created by mostly civilian (private) users, hence there is always a possibility the information they use is limited and one-sided, therefore suitable to shift narratives.

Intelligence and reconnaissance

Social media has become a powerful tool for real-time intelligence gathering. Platforms such as Twitter and TikTok allow civilians and soldiers alike to document troop movements, battle progress, and key events. The OSINT community leverages these posts to analyse military strategies, weapon deployment, and battlefield success.

For example, during the early stages of the Ukrainian crisis, photos of Russian military convoys were frequently shared on social media, allowing analysts to pinpoint troop locations and movements, sometimes even before state intelligence agencies could respond. However, misinformation (which is not intentional) and deliberate disinformation (which is intentional) can distort such data, necessitating careful cross-referencing with other sources.

Despite its utility, social media is often flooded with disinformation, especially in politically charged conflicts. While OSINT analysts strive to verify geolocated images and metadata, deepfakes and misleading content can easily distort the truth.

[12] Svetoka 2016: 90.

[13] Svetoka 2016: 71.

Disinformation campaigns can also exploit social media algorithms, making it difficult for platforms to distinguish between real and fake content.

The simplest tool for collecting open information is social media. Generation Y and Generation Z also like to joke that anyone who is not registered on one (or all) of the platforms does not really exist. In a completely clear way, the secret services lovingly use this to inform targets and set up contact networks – since the user is not necessarily a conscious user, and user awareness is generally low, so one shares information about oneself (and one's family and contact network) completely publicly.

Not surprisingly, there are also strict regulations in Hungary that the use of social media by the staff of law enforcement and defence agencies is limited (e.g. publishing a photo taken in uniform can only be published with the permission of a superior).[14]

For a similar purpose, it is forbidden to bring mobile phones into certain offices and certain locations (it is no longer a secret that applications are listening), or it is forbidden to use mobile phones when performing certain tasks in the operational area.

Besides gathering information about persons, there is much video footage posted from the frontline.

A recording which was presumably taken in the Bakhmut region during the battle is suitable for gathering intelligence and getting a more accurate picture of the events of the battles, as well as the equipment and condition of the two sides.[15]

WarLeaks channel[16] on YouTube has a designated playlist about artillery, aviation and ground operations, which serves the same OSINT/IMINT goals if used well.[17]

Target acquisition

Target designation and target selection are closely related to intelligence gathering. Many experts and volunteers (civilians) have published photos and videos of Russian troop movements on social media since the start of the war in Ukraine.

In modern warfare, target acquisition has expanded beyond traditional reconnaissance methods. For instance, civilians unknowingly assist in identifying military targets by posting geotagged images. This has occurred repeatedly during the Russian–Ukrainian war, where platforms such as Google Maps and YouTube have been utilised to identify potential targets.

While this method democratises intelligence gathering, it also raises ethical concerns. The blurred lines between civilian and military participation in intelligence activities complicate the question of accountability in warfare.

[14] Measure 4018-1/2020 of the Commander-in-Chief of the Hungarian Armed Forces on the regulation of the application and use of national defence value-creating and value-mediating internet interfaces and social media pages of the national defence organisations and their personnel.

[15] YouTube 2023. The WarLeaks YouTube channel was available at the time of writing of this study. It has since been closed [the editors].

[16] WarLeaks is an independent military blog/vlog, primarily sharing combat footage and military-related content. Established in 2014, WarLeaks focuses on providing educational and newsworthy content for military enthusiasts around the world. Its mission is to offer firsthand experiences of military events and the impact of conflicts, with a non-political stance aimed at promoting understanding rather than glorifying violence. The channel is not affiliated with any government or defence organizations. (Source: warleaks.net https://rumble.com/c/UkraineCombat)

[17] YouTube 2022.

Oryx is a blog operating on the basis of such OSINT (and IMINT), where photos taken by volunteers are constantly received and the losses of combat vehicles and equipment on the Russian and Ukrainian sides are analysed.[18]

For the purpose of similar intelligence and target identification activities, a system was created to monitor the license plates of combat vehicles coming from the Russian and Belarusian borders. Before and during the start of the war, photos of combat vehicles collected and analysed in these systems regularly appeared, for example on Twitter.[19]

An interesting example from the point of view of targeting is that after the outbreak of the first conflict in 2014, the combat radios used by the Ukrainian defence forces in the early stages of the crisis were particularly vulnerable to Russian electronic attack systems. Therefore, the Ukrainian soldiers first used their own mobile phones as an alternative for communication, which made them easy to identify and track.[20]

Social media can be a tool for this in that the published photos and videos cannot only contain important information about the area from an IMINT point of view but are often accompanied by geotagging – so we can voluntarily enter our location on the photo we want to post.

For example, this Twitter thread shows various pictures of logistics centres in Luhansk, supposedly used by Russian troops.[21]

According to the use, these are the railway hubs that are mainly used by the Russian forces, which easily makes them the next target of a possible counterattack.

Information and influence

Information warfare is now conducted on platforms that shape global narratives real-time. During the Russian–Ukrainian conflict, both sides have utilised social media to sway public perception. Ukraine has successfully employed platforms like Twitter and TikTok to portray the conflict from the perspective of its civilian victims, appealing for international support and military aid.

Conversely, Russia has used platforms for disinformation and propaganda, focusing on shaping internal narratives and influencing foreign audiences.

Ukraine effectively positioned itself as the defender in the war, portraying its civilians and cities under attack. Unlike Russia, which was seen as the aggressor, Ukraine's social media campaigns focused on humanising the conflict, sharing real-time updates of bombings, destroyed homes, and suffering families. This emotional appeal resonated deeply with Western audiences. Also, Ukraine allowed independent journalists and civilians to document the war freely, while Russia heavily censored information, used trollfarms, governmental media platforms and paid influencers. Ukrainian citizens actively posted videos and images of Russian attacks on Twitter,

[18] See: https://www.oryxspioenkop.com/search/label/Russia?&max-results=7

[19] Toler 2022.

[20] Bihaly 2022.

[21] NLwartracker 2023.

TikTok, and Telegram, increasing transparency and authenticity. These firsthand accounts were harder to dismiss as propaganda.[22]

Russia had a well-documented history of disinformation campaigns, particularly during past conflicts (e.g. Crimea 2014, U.S. election interference). This made audiences more skeptical of Russian claims. Fact-checking organisations and major social media platforms flagged or removed Russian state-backed content, further damaging Russia's credibility.[23]

The world has seen different narratives throughout time from both the eastern and the western governments. The first that may come in one's mind is the MH17 aircraft and the pro-Kremlin disinformation narratives.[24] This article shows the events and the subtle change of the narrative from 2014 to 2021 in an infographic.

The sinking of Moskva warship was a hot topic on social media. For example, on Reddit, which is a popular platform for discussing all kinds of topics, many subreddits (topics) discussed it. There were many theories (serious and humorous as well) about what was really going on.

One redditor commented that the Russian government was indeed very quiet about this event.[25]

But there was another redditor who shared their "personal experiences" during the shelling of Odessa and the sinking of Moskva. This comment also suggests that the anti-ship missiles were fired by the Russian army.[26]

Another aspect of influencing through social media is blocking content by the platform moderators. The Chinese platform, TikTok has blocked reaching Russian content from outside Russia and cut Russian users off from the outside world at the same time, thus creating a "propaganda bubble".[27]

Nonetheless, hundreds of videos were posted on TikTok, one of them is a young lady showing how to start a Russian armoured vehicle.[28] As reported by Reuters, the lady is a car mechanic and vlogger, and the video was recorded a year before the invasion of Ukraine began.

Cyberspace operations

The scope of cyberattacks continues to broaden throughout the conflict. Concurrently, according to Nissen's analysis, the social platform accounts are subjected to some form of damage during these cyberattacks. Despite the diverse presence of conflict actors across various platforms, there have been several reports of influencers' pages being compromised by hackers, yet no such incidents involving relevant war actors have been reported at the time of writing this article.

[22] Kotišová – Van der Velden 2023.

[23] Shultz – Jasparro 2022.

[24] EU vs Disinfo 2022.

[25] R/navy 2022.

[26] R/WarshipPorn – comment by U/MgLemonhead 2022.

[27] Morrison 2022.

[28] Brumfiel 2022.

Nevertheless, the utilisation of social media on the battlefield can inadvertently provide significant intelligence, and the careless and irresponsible use of geotagging can easily expose content creators to targeting. Thus, albeit indirectly, social media serves as a tool for cyberspace operations.

The rise of social media coincides with an increasing reliance on cyberspace operations in warfare. From Distributed Denial of Service (DDoS) attacks on Russian government websites to hacking social media accounts, cyberspace has become a key battleground. In particular, Ukraine's IT Army has coordinated cyberattacks via Telegram, effectively rallying civilian hackers in the fight against Russia.

The involvement of civilian actors in cyberspace operations presents significant ethical dilemmas. Non-combatants participating in DDoS attacks and cyberwarfare may be violating international law, particularly in countries where these actions are considered illegal. Moreover, social media posts can inadvertently endanger civilians, as military forces often track these activities to locate and attack cyber operations hubs.

Defence

Leaked information about operations is decreasing in an observable trend. One of the reasons for this is that OSINT-based sites like Oryx's blog at one point couldn't handle the huge amount of information that was pouring into them. On the other hand, the proper use of operational silence, especially in these extraordinary times, when everything spreads like wildfire on social media, has at least as much impact as a well-prepared disinformation campaign.

In my opinion, the defensive function of using social media as a tool of war lies precisely in this: in proper strategic communication, an integral part of which is operational silence, besides taking active and passive defence mechanisms on our information infrastructures.

The same happened to the Ukrainian forces in September, according to ISW's tweet.[29]

Command & Control (C2)

Although it can fall into the influence category, too, the next example is the deepfake video of President Zelenskyy, calling on soldiers to lay down their weapons.[30]

Deepfake videos leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content that can more easily deceive.[31]

Such attempts can easily cause the destruction of C2 within defence forces amidst the chaos of war, thereby promoting the information superiority of the opponent.

[29] ISW 2022.

[30] Thalen 2022.

[31] Kietzmann et al. 2020.

On the other hand, the non-official IT ARMY of Ukraine uses a Telegram channel not only for communicating their success, but to coordinate their operations against Russian targets.[32]

On 28th April 2022, a YouTuber with more than 260 thousand followers streamed a video, seeking help in stopping Russian propaganda, amid the Kremlin's ongoing invasion of Ukraine.[33]

The YouTuber also demonstrates how to launch a DDoS (Distributed Denial of Service) attack and partake in conducting cyberwarfare against Russia using nothing other than your own computers and a VPN connection.

DDoS attacks are easy to conduct, perhaps this is the reason we have not seen sophisticated malware attacks or extortions until the end of 2022. On the other hand, conducting any kind of cyberattacks are at least a grey zone in a legal sense, but in many countries, even DDoS attacks are criminal offenses according to their jurisdiction.[34]

Revisiting the hypothesis

H1: Social media platforms have become potent instruments in contemporary warfare, blurring the lines between traditional media and the battlefield. The study convincingly reinforces this by thoroughly investigating the multifaceted function of social media in contemporary conflicts. By exploring the intricacies of hybrid warfare and information operations, it showcases the essential integration of social media platforms into modern military tactics. Drawing from real-world instances and analysis, the essay demonstrates how social media is employed for intelligence gathering, target identification, information propagation, cyber activities, defensive measures, and command and control operations. Moreover, it critically evaluates the challenges and limitations associated with employing social media as a tool of war, including issues of bias, disinformation, and ethical considerations. Overall, the essay provides a comprehensive exploration of the intricate dynamics of modern warfare in the age of social media.

H2: The social media has been transformed in the modern conflict area, particularly in the context of the Ukrainian crisis, by illustrating how it facilitates intelligence gathering, target identification, narrative shaping, cyber operations, operational security, and coordination of actions. The essay effectively supports this hypothesis by thoroughly analysing the diverse ways in which social media is utilised within the Ukrainian crisis. The essay meticulously scrutinises real-world cases and illustrations, demonstrating how various entities leverage social media platforms to further their strategic objectives in conflicts. By elucidating the distinct roles of social media in endeavours like gathering intelligence, pinpointing targets, disseminating

[32] IT ARMY of Ukraine 2023.

[33] Boxmining 2022.

[34] Sharma 2022.

information, conducting cyber operations, implementing defence strategies, and facilitating command and control, it underscores the transformative influence of social media in contemporary warfare. Furthermore, it emphasises the necessity of nuanced comprehension in analysing the influence of social media on modern conflicts, thus reinforcing the hypothesis that social media has profoundly reshaped the landscape of warfare.

Lessons learned

The integration of social media into warfare has shifted the balance of power, allowing smaller actors, including non-state actors, to participate in modern conflicts with unprecedented ease. However, while the benefits of intelligence gathering and real-time communication are undeniable, they come with significant challenges, including the spread of disinformation and the risk of unintended civilian participation in military operations.

After corporate communication operating in the private sector, political (and even military strategic) communication also appeared on social media platforms. Now, detection and influence campaigns are not only about the individual, but enter a completely new dimension, instead of ordinary marketing goals or crimes, they are given a military-political colour.

The article highlights how social media has become a powerful tool in modern warfare. The rapid dissemination of pictures, videos, and accounts on social media platforms during the Russian invasion of Ukraine demonstrated that conflicts can now "go viral" through this medium.

Social media platforms serve as sources of open-source intelligence (OSINT), allowing military actors to gather information about targets, locations, and activities. Geotagged photos and videos shared by civilians provide valuable insights into troop movements, equipment, and conditions on the ground. Also, content posted on social media can promote, deceive, deter, and mobilise both domestic and international audiences, and by technical advancements, like deepfake, trust in information sources can be undermined, furthermore, confuse the public about the nature of events.

The article acknowledges that collecting and analysing a large volume of social media data for research is challenging. The information may be limited, biased, or one-sided, making it important to critically assess the content's accuracy and context.

Although, there will never be a single post, article or Twitter thread that can truly capture all of what's happening in Ukraine.

Collecting the data on which the research is based was difficult and had faced many obstacles. For instance, it is almost impossible to collect and classify such a large amount of information "manually", so the aim of the publication is only to give a glimpse into the fact that social media acquires a new meaning in times of war. In part, it is difficult to present the cases in full because geolocation prevents access to certain contents.

Lastly, we must realise that the use of this new tool of war to implement and support operations cannot be simply divided into categories, since these exist in multiple interdependencies in the context of hybrid warfare and information operations.

In conclusion, the study not only unravels the complexities of social media's entanglement with warfare but also offers profound insights and lessons learned. It underscores the imperative for adaptive military strategies that harness the power of social media while navigating its pitfalls, signalling a paradigm shift in the nature of modern warfare.

As the author of this essay, I emphasised the transformative role those social media platforms have assumed in contemporary warfare. Through meticulous research and analysis, I have sought to unravel the intricate dynamics of this phenomenon, shedding light on how social media has become an indispensable tool in the arsenals of military strategists and non-state actors alike.

Central to my article are the six key areas where social media intersects with warfare: intelligence and reconnaissance, target acquisition, information and influence, cyberspace operations, defence, and command and control. Through real-life cases from the Ukrainian crisis, I have illustrated how social media facilitates various aspects of military operations, from intelligence gathering to operational coordination.

However, I acknowledge the inherent limitations and challenges of using social media as a research tool in conflict zones. Issues of bias, misinformation, and ethical considerations loom large, underscoring the need for discernment and scrutiny in interpreting social media data.

In conclusion, this essay serves as a call to arms, urging policymakers, military leaders, and researchers to grapple with the complexities of social media's integration into warfare strategies. It is my hope that by shedding light on this critical issue, we can foster a more nuanced understanding of contemporary conflicts and pave the way for more effective strategies in an increasingly digitised battlefield.

Policy recommendations:

- Governments should work with social media platforms to develop better content moderation tools that can prevent the spread of disinformation without impeding free speech.
- International legal frameworks should be updated to account for the role of civilians in cyberwarfare, ensuring accountability while respecting non-combatant rights.
- Further interdisciplinary research is required to understand how artificial intelligence and deepfake technology will shape future conflicts, particularly in the realm of social media manipulation.

As for future research directions, future studies could investigate the role of non-Western social media platforms in warfare, such as Weibo or VKontakte, and explore how deepfake technologies could be integrated into future military strategies. There is also an opportunity to examine the long-term effects of social media on post-war reconstruction and international relations.

References

Bihaly, Barbara (2021): Az elektronikai hadviselés eszközei az információs és kibertérműveletek támogatásában az ukrán konfliktus példáján keresztül. *Hadmérnök,* 16(4), 101–112. Online: https://doi.org/10.32567/hm.2021.4.8

Boxmining (2022): I need your help! How you can support Ukraine with one app (DISBALANCER). *YouTube,* 28 April 2022. Online: https://www.youtube.com/watch?v=k9LwqbowGMk

Brumfiel, Geoff (2022): 4 Reasons Why Social Media Can Give a Skewed Account of the War in Ukraine. *NPR,* 19 March 2022. Online: https://www.npr.org/2022/03/19/1087265230/4-reasons-why-social-media-can-give-a-skewed-account-of-the-war-in-ukraine?t=1650349260532

Castillo, Walbert, (2015): Air Force Intel Uses ISIS 'moron' Post to Track Fighters. *CNN,* 5 June 2015. Online: https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter

EU vs Disinfo (2021): MH17: Timeline of Pro-Kremlin Disinformation narratives. *EU vs Disinfo,* 13 July 2021. Online: https://euvsdisinfo.eu/mh17-timeline-of-pro-kremlin-disinformation-narratives/

Fact Check (2022): TikTok Video Showing How to Work Russian Military Tanks Predates Invasion, 2022. *Reuters,* 2 March 2022. Online: https://www.reuters.com/article/factcheck-tiktok-tank/fact-check-tiktok-video-showing-how-to-work-russian-military-tanks-predates-invasion-idUSL1N2V520P

Haig, Zsolt (2018): *Információs műveletek a kibertérben.* Budapest: Dialóg Campus.

ISW [@TheStudyofWar] (2022): Ukrainian forces are maintaining a strict operational silence in southern Ukraine, which may appear as if Ukrainian forces are not advancing. Ukrainian forces are also likely operating in several directions in Kherson Oblast. *Twitter,* 10 September 2022. Online: https://twitter.com/TheStudyofWar/status/1568580937176211457

IT Army of Ukraine (2023): *Telegram.* Online: https://t.me/itarmyofukraine2022/990

JP-3-13 *Information Operations* (2006). Washington, D.C.: Joint Chiefs of Staff.

Kotišová, Johana – van der Velden, Lonneke. (2023). The Affective Epistemology of Digital Journalism: Emotions as Knowledge Among On-the-Ground and OSINT Media Practitioners Covering the Russo-Ukrainian War. *Digital Journalism,* 13(3), 378–397. Online: https://doi.org/10.1080/21670811.2023.2273531

Kietzmann, Jan – Lee, Linda W. – McCarthy, Ian P. – Kietzmann, Tim C. (2020): Deepfakes: Trick or Treat? *Business Horizons,* 63(2), 135–146. Online: https://doi.org/10.1016/j.bushor.2019.11.006

Measure 4018-1/2020 of the Commander-in-Chief of the Hungarian Armed Forces on the regulation of the application and use of national defence value-creating and value-mediating internet interfaces and social media pages of the national defence organisations and their personnel.

Morrison, Ryan (2022): Chinese Owned TikTok Created Alternative Universe for Russia after Ukraine Invasion. *Daily Mail,* 14 April 2022. Online: https://www.dailymail.co.uk/sciencetech/article-10718887/Chinese-owned-TikTok-created-alternate-universe-Russia.html

Nissen, Thomas E. (2015): *#TheWeaponizationOfSocialMedia.* Coppenhangen: Royal Danish Defence College.

NLwartracker [@NLwartracker] (2023): 1/15 I have been working on unraveling the Russian logistics networks in the Luhansk area since the beginning of Jan. when different geolocated videos showed convoy's of armoured vehicles moving towards the frontlines in Luhansk & Donetsk. *Twitter,* 18 February 2023. Online: https://twitter.com/NLwartracker/status/1627047617938223106?fbclid=IwAR07SBr-NuQiUjG0SEF6bf3YkwkB1yC3vFI7XUt5jjClCu5UqHcctKrkTlRE

ORYX (2023): Russia. *Oryx,* 24 June 2023. Online: https://www.oryxspioenkop.com/search/label/Russia?&max-results=7

R/navy (2022): Explanation of what happened to the cruiser "Moscow". *reddit,* 2022. Online: https://www.reddit.com/r/navy/comments/u4fsul/explanation_of_what_happened_to_the_cruiser_moscow/

R/WarshipPorn – comment by U/MgLemonhead (2022): Rip, mighty one. admirals did not improve the fire extinguishing system and they paid for it. this photo was taken at April 10, 4 days ago. [1280*960]. *reddit,* 2022. Online: https://www.reddit.com/r/WarshipPorn/comments/u34fr5/comment/i4nbbub/

Sharma, Ax (2022): A YouTuber is encouraging you to DDoS Russia – How Risky is This? *Bleeping Computer,* 1 May 2022. Online: https://www.bleepingcomputer.com/news/security/a-youtuber-is-encouraging-you-to-ddos-russia-how-risky-is-this/

Schultz, Daniel – Jasparro, Christopher (2022): How Does Russia Exploit History and Cultural Heritage for Information Warfare? Recommendations for NATO. *Think Tank Policy Brief.* Online: https://acthinktank.scholasticahq.com/article/118601-how-does-russia-exploit-history-and-cultural-heritage-for-information-warfare-recommendations-for-nato

Svetoka, Sanda (2016): *Social Media as a Tool of Hybrid Warfare.* Riga: NATO Strategic Communications Centre of Excellence.

Thalen, Mikael [@MikaelThalen] (2022): A deepfake of Ukrainian president Volodymyr Zelensky calling on his soldiers to lay down their weapons was reportedly uploaded to a hacked Ukrainian news website today, per @shayan86 pic.twitter.com/txlryecgy4. *Twitter,* 16 March 2022. Online: https://twitter.com/MikaelThalen/status/1504123674516885507?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504123674516885507%7Ctwgr%5E8a277957fe170d7ef663b92d1379fc1b9f7f0e5d%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.npr.org%2F2022%2F03%2F19%2F1087265230%2F4-reasons-why-social-media-can-give-a-skewed-account-of-the-war-in-ukraine

Toler, Aric (2022): Tracking Russian Military Vehicles on the Move. *Bellingcat,* 8 February 2022. Online: https://www.bellingcat.com/resources/how-tos/2022/02/08/tracking-russian-military-vehicles-on-the-move/

YouTube (2022): Ukraine War: Russian Missile Intercepted by Ukrainian Air Defense. Online: https://www.youtube.com/watch?v=ioxN760OX6U&list=PLQo8IaJoevFtcICk6IR-GivMPZH3FIcYs

YouTube (2023): Intense GoPro Combat Footage of Trench Battle in Ukraine #ukrainewar. Online: https://www.youtube.com/watch?v=2yB8jKUmXj0&list=PLQo8IaJoevFsfTsNEwXO5SUF0hSuw7VLR&index=1&t=0s